



DEPARTMENT OF DEFENSE
Defense Contract Management Agency

INSTRUCTION

Cybersecurity/Information Assurance (IA)

Information Technology
OPR: DCMA-IT

DCMA-INST 815
July 10, 2014

1. PURPOSE. This Instruction:

- a. Establishes cybersecurity/information assurance (IA) policy, mandates, roles, responsibilities, and procedures for implementing the DCMA Cybersecurity (i.e., IA) Program.
- b. Is established in compliance with DoD Directive (DoDD) 5105.64, “Defense Contract Management Agency (DCMA)” (Reference (a)) and DoD Instruction (DoDI) 8500.01, “Cybersecurity” (Reference (b))
- c. Adopts the term “cybersecurity” as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (c)) to be used throughout DoD instead of the term “information assurance (IA).”

2. APPLICABILITY. This Instruction applies to all DCMA activities.

3. MANAGERS' INTERNAL CONTROL PROGRAM (MICP). In accordance with (IAW) DCMA Instruction (DCMA-INST) 710, “Managers’ Internal Control Program” (Reference (d)), this Instruction is subject to evaluation and testing. This instruction contains management control provisions and identifies key management controls that must be evaluated. The MICP process flow and controls are located on the policy resource web page.

4. RELEASABILITY – UNLIMITED. This Instruction is approved for public release.

5. PLAS CODE. B212 – Security (Systems/Communication Support)

6. POLICY RESOURCE WEB PAGE. <https://home.dcma.mil/policy/815r>

7. EFFECTIVE DATE. By order of the Director, DCMA, this Instruction is effective July 10, 2014, and all applicable activities shall be fully compliant within 60 days from this date.

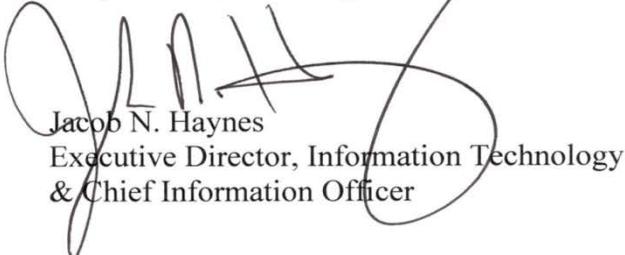

Jacob N. Haynes
Executive Director, Information Technology
& Chief Information Officer

TABLE OF CONTENTS

REFERENCES.....	4
-----------------	---

CHAPTER 1 –CYBERSECURITY/INFORMATION ASSURANCE PROGRAM

1.1. Overview.....	7
--------------------	---

CHAPTER 2 – ROLES AND RESPONSIBILITIES

2.1. Director, DCMA	14
2.2. Executive and Center Directors and Commanders/Directors of Contract Management Offices	17
2.3. Chief Information Officer (CIO)	17
2.4. Designated Approval Authority (DAA).....	18
2.5. Information Technology Senior Leadership Team (IT-SLT)	18
2.6. Director, Information Assurance (Cybersecurity) Division.....	19
2.7. Senior Information Security Officer (SISO).....	19
2.8. Information Assurance (Cybersecurity) Workforce	19
2.9. Information System Owner (ISO).....	20
2.10 Data Owner/Information Owner	20
2.11. Certification Agent (CA)	20
2.12. Managers/Supervisors	20
2.13. General User	21
2.14. Lead-IT Accountable Property Officer (APO)	22
2.15. DCMA FISMA Coordinator	22

CHAPTER 3 – PROCESS

3.1. Certification and Accreditation (C&A)/Risk Management Framework (RMF).....	24
3.2. FISMA	27
3.3. Computer Network Defense (CND)	28
3.4. DOD Information.....	30
3.5. Cybersecurity Workforce.....	37
3.6. Mission Partners.....	37
3.7. Information Technology (IT)	39

FIGURES

Figure 1 Three-Tiered Risk Management Approach	10
Figure 2 NIST 800-53 Security Control Families.....	11
Figure 3 Risk Management Framework	25
Figure 4 RMF and the DoD Acquisition Lifecycle	27
Figure 5 DoD Information Technology	40

TABLES

Table 1	Investigative Levels for User with IA Management Access to DoD Unclassified Systems	35
Table 2	Investigative Levels for DoD Information System Users Responsible for PKI Certificate Issuance	37

GLOSSARY

Definitions	46
Acronyms	56

REFERENCES

- (a) DoD Directive 5105.64, “Defense Contract Management Agency (DCMA),” January 10, 2013
- (b) DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014
- (c) National Security Presidential Directive-54/Homeland Security Presidential Directive-23, “Cybersecurity Policy,” January 8, 2008
- (d) DCMA-INST 710, “Managers’ Internal Control Program,” April 21, 2014
- (e) DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014
- (f) Section 35 of Title 44, United States Code (also known as “Coordination of Federal Information Policy”)
- (g) Section 11331 of Title 40, United States Code
- (h) Section 20 of Title 15, United States Code
- (i) Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” February 8, 1996
- (j) National Institute of Standards and Technology Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations,” current edition
- (k) DoD Directive 8570.01, “Information Assurance (IA) Training, Certification, and Workforce Management,” August 15, 2004
- (l) DoD Instruction O-8530.2, “Support to Computer Network Defense (CND),” March 9, 2001
- (m) DoD Manual 5200.01, Volume 3, “DoD Information Security Program: Protection of Classified Information,” February 24, 2012, as amended
- (n) DoD Manual 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information (CUI),” February 24, 2012
- (o) DoD 5220.22-M, “National Industrial Security Program Operating Manual,” February 28, 2006, as amended
- (p) DoD Regulation 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007
- (q) Sections 791, 794, and 794d of Title 29, United States Code
- (r) National Institute of Standards and Technology Special Publication 800-34, Revision 1, “Contingency Planning Guide for Federal Information Systems,” current edition
- (s) DoD Regulation 5200.2-R, “Personnel Security Program,” January 1, 1987, as amended
- (t) DoD Manual 5200.01, Volume 1, “DoD Information Security Program: Overview, Classification, and Declassification,” February 24, 2012
- (u) DoD Regulation 5200.08-R, “Physical Security Program,” April 9, 2007, as amended
- (v) DoD Manual 5200.01, Volume 2, “DoD Information Security Program: Marking of Classified Information,” February 24, 2012, as amended
- (w) DoD Regulation 5220.22-R, “Industrial Security Regulation,” April 12, 1985
- (x) DoD 8570.01-M, “Information Assurance Workforce Improvement Program,” December 19, 2005, as amended
- (y) DCMA-INST 552, “Information Security Program,” October 29, 2013
- (z) Section 4531 of Title 44, United States Code
- (aa) Executive Order 12356, “National Security Information”
- (ab) DoD Instruction 8560.01, “Communications Security (COMSEC) Monitoring and Information Assurance Readiness Testing,” October 7, 2007

- (ac) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008, as amended
- (ad) DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011
- (ae) DCMA-INST 522, "Public Affairs," August 2, 2012
- (af) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
- (ag) DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012
- (ah) DoD Regulation 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (ai) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009
- (aj) DoD Regulation 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007
- (ak) DCMA-INST 556, "Operations Security," March 31, 2011
- (al) DCMA-INST 557, "Physical Security," August 31, 2011
- (am) DCMA-INST 806, "Networks and Application Access," June 4, 2013
- (an) NTI SSP No. 200, "National Policy on Controlled Access Protection," July 15, 1987
- (ao) DoD Regulation 5500.7-R, "Joint Ethics Regulation (JER)," March 23, 2006
- (ap) DCMA-INST 555, "Personnel Security," October 22, 2012
- (aq) DoD Instruction 1400.25, Volume 731, "DoD Civilian Personnel Management System: Suitability and Fitness Adjudication For Civilian Employees," August 24, 2012
- (ar) Chairman of the Joint Chiefs of Staff Instruction 6510.01, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, as amended
- (as) Executive Order 12968, "Access to Classified Information," August 2, 1995
- (at) DoD Instruction 2030.08, "Implementation of Trade Security Controls (TSC) for Transfers of DoD U.S. Munitions List (USML) and Commerce Control List (CCL) Personal Property to Parties Outside DoD Control," May 23, 2006
- (au) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
- (av) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987
- (aw) Chairman of the Joint Chiefs of Staff Instruction 6211.02, "Defense Information System Network (DISN) Responsibilities," current edition
- (ax) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
- (ay) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," July 10, 2008
- (az) DoD Directive 5530.3, "International Agreements," June 11, 1987, as amended
- (ba) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990
- (bb) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
- (bc) Section 2224 of Title 10, United States Code
- (bd) DCMA-INST 810, "DCMA-IT Acquisitions – Non-Programmed Acquisitions Valued at \$3,000 Or Below," April 2, 2013
- (be) DoD CIO Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile

- Computing Devices and Removable Storage Media,” 3 July 2007
- (bf) DoD Instruction 1035.01, “Telework Policy,” April 4, 2012
- (bg) National Institute of Standards and Technology Special Publication 800-114, “Users Guide to Securing External Devices for Telework and Remote Access,” current edition
- (bh) DoD Instruction 5230.29, “Security and Policy Review of DoD Information for Public Release,” January 8, 2009.
- (bi) Committee on National Security Systems Instruction Number 4009, “National Information Assurance (IA) Glossary,” April 26, 2010, as amended

CHAPTER 1

CYBERSECURITY/INFORMATION ASSURANCE PROGRAM

1.1. OVERVIEW. The DCMA Cybersecurity (i.e., IA) Program is the agency's unified approach to protect unclassified, sensitive, and classified information stored, processed, accessed, and transmitted by DCMA Information Systems (IS). The DCMA Cybersecurity (i.e., IA) Program is hereby established to consolidate and focus DCMA efforts in securing information, including its associated systems and resources, in order to increase the level of trust of this information and the originating source.

NOTE 1. On March 12, 2014, DoD released DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)" (Reference (e)) establishing the RMF for DoD IT establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT.

NOTE 2. As per DoDI 8510.01 (Reference (e)), DoD has 3 years and 6 months from March 12, 2014 to be fully transitioned to RMF for existing IT systems managed under DIACAP. All new systems or systems just starting the DIACAP life-cycle are required to implement RMF as per the DoDI 8510.01 (Reference (e)).

NOTE 3. On March 14, 2014, DoD released DoDI 8500.01 (Reference (b)) hereby removing the term "information assurance" and replacing it with the term "cybersecurity." DoDI 8500.01 (Reference (b)) reissues and renames DoDD 8500.01, "Information Assurance (IA)" as DoDI 8500.01 "Cybersecurity" (Reference (b)).

NOTE 4. This DCMA policy has incorporated elements of the RMF as the first stages of transition from DIACAP to RMF; however, the terms from DIACAP are still used throughout this Instruction. An update to this Instruction is planned for 2015 which will more fully cover the RMF and eliminate, where appropriate, the DIACAP terminologies and references.

1.1.1. DoDI 8500.01 (Reference (b)) and section 35 of Title 44, "Federal Information Security Management Act (FISMA) of 2002" (Reference (f)) mandate that organizations establish cybersecurity (i.e., IA) programs that institute processes and metrics to ensure all applicable laws, regulations, and directives are followed to include metrics that will provide leadership with situational awareness of triggers to identify compliance or potential issues. The purpose of the DCMA Cybersecurity (i.e., IA) Program is to ensure that IT can be used in a way that allows mission owners and operators to have confidence in the confidentiality, integrity, and availability of IT and DCMA information, and to make choices based on that confidence.

1.1.1.1. **Cybersecurity** ensures prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its integrity, confidentiality, availability, authentication, and nonrepudiation.

1.1.1.1.1. **Integrity** ensures guarding against improper information modification or destruction, and includes ensuring information **nonrepudiation** and authenticity.

1.1.1.1.2. **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy, sensitive, official use only, and proprietary information (Controlled Unclassified Information (CUI)).

1.1.1.1.3. **Availability** ensures timely and reliable access to and use of information.

1.1.1.1.4. **Authentication** provides security measures designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

1.1.1.1.5. **Nonrepudiation** provides the assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

1.1.1.1.6. **Information Technology (IT) Information Systems (IS)** includes all DoD IT that receive, process, store, display, or transmit DoD information. These technologies are broadly grouped as DoD IS, platform IT (PIT), IT services, and IT products. This includes IT supporting research, development, test and evaluation (RDT&E), and DoD controlled IT operated by a contractor or other entity on behalf of the DoD.

1.1.1.2. The DCMA Cybersecurity (i.e., IA) Program provides for development and maintenance of minimum controls (see Figure 2) required to protect Federal information and ISs. It will include a series of DCMA policies, principles, standards, and guidelines on information security IAW section 11331 of Title 40, United States Code (U.S.C.) (Reference (g)).

1.1.1.3. As part of the DCMA Cybersecurity (i.e., IA) Program, DCMA-IT shall develop security controls to minimize the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of:

1.1.1.3.1. DCMA data, which includes information collected or maintained by or on behalf of the agency.

1.1.1.3.2. DCMA IT systems used or operated by the Agency or by a contractor of the Agency or other organization on behalf of the Agency.

1.1.1.3.3. National Security Systems, if DCMA manages or procures the development or operation of National Security Systems as defined in section 20 of Title 15, U.S.C. "National Institute of Standards and Technology Act" ((Reference (h)) with agencies and offices, DCMA will assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems.

1.1.2. The goal of the DCMA Cybersecurity (i.e., IA) Program is to provide a holistic approach to information security and risk management by providing an environment with the

breadth and depth of security controls necessary to fundamentally strengthen their ISs and the environments in which those systems operate, contributing to systems that are more resilient in the face of cyber-attacks and other threats. This “**Build It Right**” strategy will be coupled with a variety of security controls for “**Continuous Monitoring**” to provide near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions. The ultimate objective is to conduct the day-to-day operations of the organization and accomplish the organization’s stated missions and business functions with what the Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources” (Reference (i)) defines as adequate security, or security commensurate with risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

1.1.3. Achieving adequate information security for DCMA’s mission/business processes and ISs is a multifaceted undertaking that requires:

1.1.3.1. Clearly articulated security requirements and security specifications.

1.1.3.2. Well-designed and well-built IT products based on state-of-the-art hardware, firmware, and software development processes.

1.1.3.3. Sound systems/security engineering principles and practices to effectively integrate IT products into organizational ISs.

1.1.3.4. Sound security practices that are well documented and seamlessly integrated into the training requirements and daily routines of organizational personnel with security responsibilities.

1.1.3.5. Continuous monitoring of organizations and ISs to determine the ongoing effectiveness of deployed security controls; changes in ISs and environments of operation; and compliance with legislation, directives, policies, and standards.

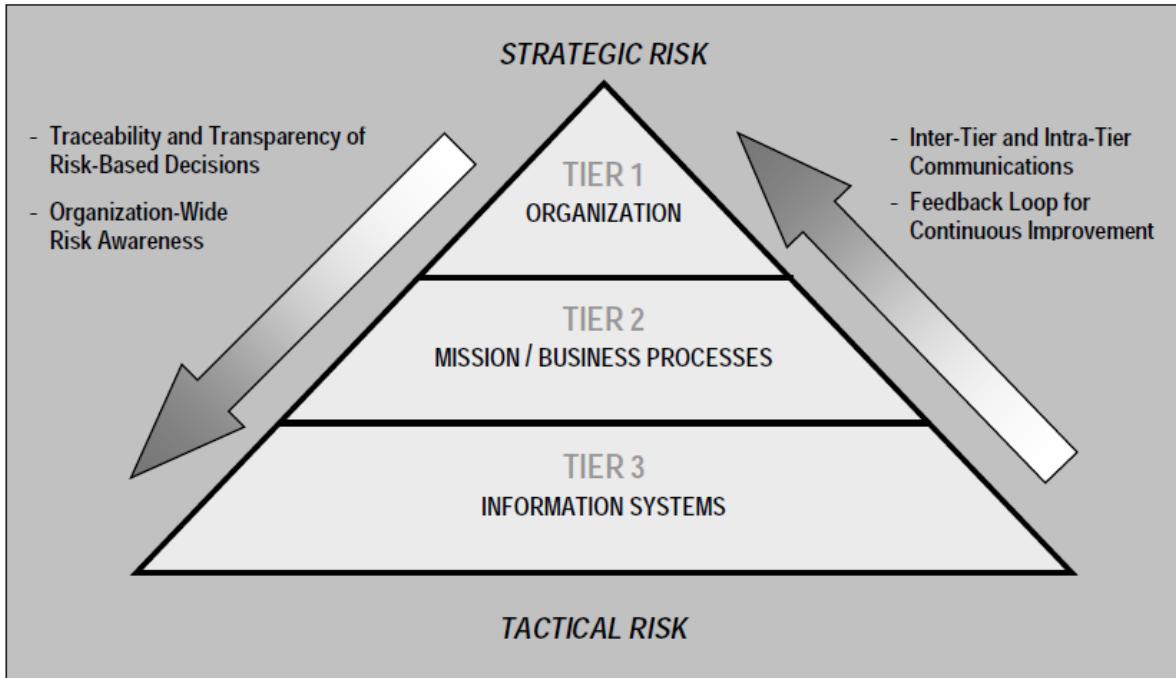
1.1.3.6. Information security planning and system development life-cycle management.

1.1.4. From an engineering viewpoint, information security is just one of many required operational capabilities for ISs that support organizational mission/business processes, capabilities that must be funded by organizations throughout the system development life-cycle in order to achieve mission/business success. It is important that DCMA realistically assess the risk to its operations and assets, individuals, other customers, and the Nation arising from mission/business processes and by placing ISs into operation or continuing operations. Accurate assessment of risk requires an understanding of threats to and vulnerabilities within organizations and the likelihood and potential adverse impacts of successful exploitations of such vulnerabilities by those threats. Finally, information security requirements must be satisfied with the full knowledge and consideration of the risk management strategy.

1.1.5. Integrated Organization-Wide Risk Management. Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization. To integrate the

risk management process throughout DCMA and more effectively address mission/business concerns, a three-tiered approach will be employed that addresses risk at the organization level, mission/business process level, and IS level. The risk management process is carried out across the three tiers with the overall objective of continuous improvement in DCMA's risk-related activities and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization. Figure 1 illustrates the three-tiered approach to DCMA cybersecurity (i.e., IA) risk management.

Figure 1. Three-Tiered Risk Management Approach



1.1.5.1. Risk management at Tier 1 addresses risk from an organizational perspective. As part of the feedback loop, Tier 1 risk management is informed and influenced by risk decisions made in Tiers 2 and 3. A comprehensive IS security governance structure is established that provides assurance that IS security strategies are aligned with and support mission and business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility.

1.1.5.2. Tier 2 addresses risk from a mission and business process perspective and is guided by the risk decisions at Tier 1, and informed and influenced by risk decisions made in Tier 3. The activities at Tier 2 begin with the design, development, and implementation of the mission and business processes defined at Tier 1.

1.1.5.3. Tier 3 addresses risk from an IS and PIT system perspective and is guided by the risk decisions at Tiers 1 and 2. Though the need for specific protections is identified at Tiers 1 and 2, it is at Tier 3 where the information protections are applied to the system and its environment of operation for the benefit of successfully enabling mission and business success. Information protection requirements are satisfied by the selection and implementation of

appropriate security controls. Security controls are implemented at Tier 3 by common control providers, IS owners (ISO), or project managers (PM), and risk-based authorization decisions are granted by the designated approving authority (DAA).

1.1.6. Security controls are defined within cybersecurity (i.e., IA) to apply management, operations, and technical controls (i.e., safeguards or counter measures) prescribed for an IS to protect the confidentiality, integrity, and availability of the system and its information. Specific security controls are grouped into security control families as detailed in the National Institute of Standards and Technology (NIST) Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations” (Reference (j)). Figure 2 details the families and the two letter identifier that is used in labeling the technical and policy controls associated them. The specific controls will be detailed in another policy that will be released by IT. Each IT system is required to have the specific security controls detailed and determined as part of the system development planning cycle. It is infinitely harder to attempt to “bolt-on” security controls after system development. The preferred and most efficient way to secure a system is to “bake-in” the controls during the planning stages and prior to system development or acquisition.

Figure 2. NIST 800-53 Security Control Families

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

1.1.6.1. The challenge for cybersecurity (i.e., IA) is that in order to protect IT systems and data that resides on, is stored by, is manipulated by, or is transported DCMA is required to adequately mitigate the risk arising from use of information and ISs in the execution of missions and business functions. DCMA must determine the most cost-effective, appropriate set of security controls, which if implemented and determined to be effective, would mitigate risk while complying with security requirements defined by applicable federal laws.

NOTE. There is no one correct set of security controls that addresses all organizational security concerns in all situations.

1.1.6.2. Selecting the most appropriate set of security controls for a specific situation or IS to adequately mitigate risk is an important task that requires a fundamental understanding of organizational mission/business priorities, the mission and business functions the ISs will support, and the environments of operation where the systems will reside. With that

understanding, DCMA can demonstrate how to most effectively assure the confidentiality, integrity, and availability of organizational information and ISs in a manner that supports mission/business needs while demonstrating due diligence. Selecting, implementing, and maintaining an appropriate set of security controls to adequately protect the ISs employed by organizations requires strong collaboration with system owners to understand ongoing changes to missions/business functions, environments of

1.1.7. Scope. The DCMA Cybersecurity (i.e., IA) Program will be comprised of certification and accreditation (C&A)/RMF, computer network defense (CND), DoD information, mission partners, and IT.

NOTE: The DCMA Cybersecurity (i.e., IA) Program does not extend to IT systems classified as or include access privileges to special access programs or compartmentalized data. The DCMA Cybersecurity (i.e., IA) Program covers all unclassified IT systems and unclassified electronic data. The DCMA Cybersecurity (i.e., IA) Program also includes all DCMA IT systems classified as Secret or below and electronic data that is Secret or below.

1.1.7.1. The DCMA has a crucial responsibility to protect and defend its information and supporting IT. DoD information is shared across a Global Information Grid (GIG) that is inherently vulnerable to exploitation and denial of service. Factors that contribute to its vulnerability include: increased reliance on commercial IT and services, increased complexity and risk propagation through interconnection, the extremely rapid pace of technological change, a distributed and non-standard management structure, and the relatively low cost of entry for adversaries.

1.1.7.2. Complete confidence in the trustworthiness of IT, users, and interconnections cannot be achieved; therefore, DCMA must embrace a risk management approach that balances the importance of the information and supporting technology to DoD missions against documented threats and vulnerabilities, the trustworthiness of users and interconnecting systems, and the effectiveness of cybersecurity (i.e., IA) solutions.

1.1.7.3. The DCMA Cybersecurity (i.e., IA) Program is predicated upon six essential competencies that are the hallmark of any successful risk management program. They include:

- The ability to assess security needs and capabilities
- The ability to develop a purposeful security design or configuration that adheres to a common architecture and maximizes the use of common services
- The ability to implement required controls or safeguards
- The ability to test and verify
- The ability to manage changes to an established baseline in a secure manner
- Layered technical defenses

1.1.7.4. Even the best available IT products have inherent weaknesses. Eventually an adversary will likely find an exploitable vulnerability. An effective countermeasure is the deployment of multiple defense mechanisms between the adversary and the target. In order to

reduce the likelihood or affordability of successful attacks, each mechanism should present unique obstacles and include both protection and detection measures.

1.1.8. Annual Independent Evaluation. DCMA shall have an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

CHAPTER 2

ROLES AND RESPONSIBILITIES

2.1. DIRECTOR, DCMA. The Director, DCMA oversees the Agency's information security policies and practices; ensuring that policies are developed, principles are established, standards are implemented and enforced, security guidelines are used and validated, and the Agency remains compliant with standards promulgated under section 11331 of title 40, U.S.C. (Reference (g)). The Director, DCMA shall:

2.1.1. Ensure information security protections are commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained on behalf of DCMA, and on ISs used or operated by an agency or by a contractor of an agency or other organization on behalf on an agency.

2.1.2. Ensure that cybersecurity (i.e., IA) requirements are addressed and visible in all capability portfolios, IT life-cycle management processes, and investment programs incorporating IT.

2.1.3. Ensure that senior agency officials provide information security for the information and ISs that support the operations and assets under their control, to include:

2.1.3.1. Assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or ISs.

2.1.3.2. Determining the levels of information security appropriate to protect such information and ISs IAW standards promulgated under section 11331 of title 40, U.S.C. (Reference (g)), for information security classifications and related requirements.

2.1.4. Ensure policies and procedures are implemented to cost-effectively reduce risks to an acceptable level.

2.1.5. Ensure DCMA periodically tests and evaluates information security controls and techniques to confirm that they are effectively implemented.

2.1.6. Appoint a chief information officer (CIO) and delegate to the CIO the authority to ensure compliance with the requirements imposed on DCMA under this Instruction.

2.1.7. Appoint authorizing officials (i.e., DAAs) according to DoDI 8500.01 (Reference (b)) and ensure they accredit each DCMA system according to DoDI 8510.01 (Reference (e)).

NOTE: As of March 12, 2014, all new systems will be accredited according to DoDI 8510.01 (Reference (e)) and by August 2017 all DCMA systems will be accredited according to DoDI 8510.01 (Reference (e)).

2.1.8. Ensure DCMA establishes, resources, and implements cybersecurity (i.e., IA) training and certification programs for all DCMA personnel IAW DoDD 8570.01, “Information Assurance Training, Certification, and Workforce Management” (References (k)).

2.1.9. Ensure DCMA personnel develop and maintain an inventory of major ISs (including major national security systems) operated by or under the control of DCMA to include identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of DCMA. Inventory must be updated at least annually.

2.1.10. Ensure independent evaluation of DCMA Cybersecurity (i.e., IA) Program and practices is performed annually and DCMA-IT provides a report of outcome.

2.1.11. Ensure DCMA IS and PIT systems are categorized according to the guidelines provided in this Instruction.

2.1.12. Verify that a PM or system manager is appointed for all ISs and PIT systems.

2.1.13. Ensure Agency personnel develop and issue guidance for PIT systems that reflects DCMA operational and environmental demands as needed.

2.1.14. Ensure DoD information technologies under their authority comply with the RMF as per DoDI 8510.01 (Reference (e)).

2.1.15. Ensure Agency personnel operate only authorized ISs and PIT systems (i.e., those with a current authorization to operate (ATO), interim authorization to test, or interim authorization to operate).

2.1.16. Ensure personnel engaged in or supporting the RMF are appropriately trained and possess professional certifications consistent with DoDI 8510.01 (Reference (e)) and supporting issuances as per DoDI 8510.01 (Reference (e)).

2.1.17. Ensure DCMA ISOs appoint user representatives (UR) for DoD IS and PIT systems under the DoD Component’s purview.

2.1.18. Ensure participation in the RMF Technical Advisory Group as per DoDI 8510.01 (Reference (e)). This will ensure that DCMA issues and requirements are discussed in this most senior level governance board.

2.1.19. Ensure that contracts and other agreements include specific requirements IAW DoDI 8500.01 (Reference (b)).

2.1.20. Provide for vulnerability mitigation and incident response and reporting capabilities in order to:

2.1.20.1. Comply with mitigations as directed by Commander, U.S. Strategic Command (USSTRATCOM) orders, or other directives such as alerts and bulletins and provide support to cyberspace defense, IAW DoDI O-8530.2, “Support to Computer Network Defense (CND)” (Reference (l)).

2.1.20.2. Limit damage and restore effective service following an incident.

2.1.20.3. Collect and keep audit data to support technical analysis relating to misuse, penetration, or other incidents involving IT under their purview, and provide this data to appropriate law enforcement (LE) or other investigating agencies.

2.1.20.4. Establish procedures to ensure prompt management action and reporting IAW, DoD Manual (DoDM) 5200.01, Volume 3 “DoD Information Security Program: Protection of Classified Information” (Reference (m)) for an actual or potential compromise of classified information; DoDM 5200.01, Volume 4 “DoD Information Security Program: Protection of Classified Information” (Reference (n)) for an actual or potential unauthorized disclosure of CUI (e.g., proprietary information, LE information); DoD 5220.22-M, “National Industrial Security Program Operating Manual” (Reference (o)) when such losses occur on cleared contractor systems; or DoD Regulation 5400.11-R “Department of Defense Privacy Program” (Reference (p)) for a loss or unauthorized disclosure of personally identifiable information (PII) or other Privacy Act information.

2.1.21. Ensure that appropriate notice of privacy rights and monitoring policies are provided to all individuals accessing DoD Component-owned or controlled DoD ISs.

2.1.22. Ensure that cybersecurity solutions do not unnecessarily restrict the use of assistive technology by individuals with disabilities or access to or use of information and data by individuals with disabilities IAW sections 791, 794, and 794d of Title 29, U.S.C. (Reference (q)).

2.1.23. Develop DoD IS contingency plans and conduct exercises to recover IS services following an emergency or IS disruption using guidance found in NIST SP 800-34 “Contingency Planning Guide for Federal Information Systems” (Reference (r)).

2.1.24. Ensure individual and organization accountability within organizations under their purview, including:

2.1.24.1. Hold commanders, ISOs, DAAs, information assurance (i.e., cybersecurity) managers (IAM), system owners, PMs, project and application leads, supervisors, and system administrators (SA) responsible and accountable for the implementation of DoD security requirements IAW this Instruction; DoD Regulation 5200.2-R “Personnel Security Program” (References (s)); DoDM 5200.01, Volume 3 (Reference (m)); DoDM 5200.01, Volume 4 (Reference (n)); DoDM 5200.01, Volume 1, “DoD Information Security Program: Overview, Classification, and Declassification” (Reference (t)); DoD Regulation 5200.08-R, “Physical Security Program” (Reference (u)); DoDM 5200.01, Volume 2, “DoD Information Security Program: Marking of Classified Information” (Reference (v)); DoD Regulation 5220.22-R, “Industrial Security Regulation” (Reference (x)); and supplemental DoD Component guidance.

Personnel filling positions with privileged access must be qualified and sign a Statement of Acceptance of Responsibilities IAW DoD 8570.01-M, “Information Assurance Workforce Improvement Program (Reference (x)).

2.1.24.2. Ensure that military and civilian personnel are considered for administrative or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place at risk DoD information by not ensuring implementation of DoD security requirements IAW this Instruction, other DoD 8500 series directives and instructions, DoD 5200 series instructions and publications, and supplemental DoD Component policies and procedures.

2.2. EXECUTIVE AND CENTER DIRECTORS AND COMMANDERS/DIRECTORS OF CONTRACT MANAGEMENT OFFICES (CMO). The Executive and Center Directors and Commander/Directors of CMOs shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

2.2.1. Participate collectively with the CIO in the enterprise planning, acquisition, and operation of IS procured for their respective component.

2.2.2. Establish information classification, sensitivity, and need-to-know for DCMA Component-specific information IAW DCMA-INST 552, “Information Security Program” (Reference (y)).

2.2.3. Operate and maintain systems within their command or activity per this Instruction.

2.2.4. Incorporate and define requests for new systems or changes to existing systems, including security requirements necessary for the system’s concept of operation. Once validated, include these security requirements into the system design as defined in procurement contracts. Address the addition of IT/IA personnel (such as SAs or network security managers needed to operate the new or expanded system or network) as part of the development cost of stated system or network.

2.3. CHIEF INFORMATION OFFICER (CIO). The CIO shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

2.3.1. Establish and oversee DCMA’s Cybersecurity (i.e., IA) Program.

2.3.2. Ensure the effective implementation of DCMA’s Cybersecurity (i.e., IA) Program and evaluate the performance of major DCMA components, as well as, carrying out the information resource management functions of DCMA.

2.3.3. Implement IT policies, principles, standards, and guidelines with respect to all areas of information resources.

2.3.4. Review any requested exemptions to policy and signing approved exemptions.

2.3.5. Report annually to the agency head the effectiveness of DCMA's Cybersecurity (i.e., IA) Program including progress of remedial actions.

2.3.6. Designate a Senior Agency Information Security Officer (SISO).

2.3.7. Ensure independent evaluation of DCMA information security program and practices is performed annually and report of the outcome provided to the Director, DCMA.

2.3.8. Develop and maintain cybersecurity policies, procedures, and control techniques to address all applicable requirements.

2.4. DESIGNATED APPROVAL AUTHORITY (DAA). The DAA shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

2.4.1. Issue ATO or other accreditation for an IS that has an acceptable level of risk to agency operations, assets, or individuals.

2.4.2. Issue Deny Authority To Operate for an IS with unacceptable security risks and will order the affected assets blocked or disconnected from the network IAW DCMA guidance, as necessary.

2.4.3. Accept risk on behalf of the Agency.

2.4.4. Grant DCMA ISs under his or her purview formal accreditation to operate according to the DoD cybersecurity (i.e., IA) C&A process DoDI 8510.01 (Reference (e)).

2.5. INFORMATION TECHNOLOGY SENIOR LEADERSHIP TEAM (IT-SLT). The IT-SLT shall:

2.5.1. Implement cybersecurity (i.e., IA) requirements within their respective functional areas.

2.5.2. Develop, coordinate, supervise, execute, and allocate the RDT&E procurement resources in support of cybersecurity (i.e., IA) program requirements as required in their functional area.

2.5.3. Participate collectively with other cybersecurity (i.e., IA) stakeholders in the enterprise planning, acquisition, and operation of cybersecurity (i.e., IA) strategies.

2.5.4. Integrate approved cybersecurity (i.e., IA) tools, doctrine, procedures, and techniques into all ISs under their purview.

2.5.5. Ensure the C&A package is submitted to the DCMA certification authority (CA) in sufficient time for a review and operational cybersecurity (i.e., IA) risk recommendation in support of DAA authorization decision prior to operations or tests on a live network or with live DCMA data.

2.5.6. Identify personnel and procedures at all organizational and subordinate levels, as required, to implement a Configuration Management Board or Configuration Control Board to effect control and management mechanisms on all ISs, devices, configurations, and cybersecurity (i.e., IA) implementations. Include cybersecurity (i.e., IA) personnel as members of the board.

2.6. DIRECTOR, INFORMATION ASSURANCE (CYBERSECURITY) DIVISION.

DCMA CIO shall appoint Information Assurance (Cybersecurity) Director as the SISO. The Director, Information Assurance (Cybersecurity) Division, shall abide by and support the responsibilities in Section 2.1 of this Instruction and serves as principal advisor to the DCMA Director and CIO for the DCMA Cybersecurity (i.e., IA) Program.

2.7. SENIOR AGENCY INFORMATION SECURITY OFFICER (SISO). The SISO shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

2.7.1. Ensure C&A of DCMA ISs is accomplished IAW minimum security control guidelines based on NIST 800-53 (Reference (j)) and other guidelines.

2.7.2. Provides the agency's AOs with the most objective information possible to make an informed, risk-based accreditation decision.

2.7.3. Recommend corrective actions to reduce or eliminate vulnerabilities in the IS.

2.7.4. Ensure independent evaluation of DCMA Cybersecurity (i.e., IA) Program and practices is performed annually.

2.7.5. Prepare a report for the Director and CIO of independent evaluation results and recommendations.

2.7.6. Lead an office with the mission and resources to assist in ensuring Agency compliance with this Instruction.

2.8. INFORMATION ASSURANCE (CYBERSECURITY) WORKFORCE. Cybersecurity (i.e., IA) workforce personnel include but are not limited to SAs or Network Administrators (NA), Information Assurance Managers (IAM), Information Assurance Officers (IAO), CAs, ISOs, AOs, and data owners. DCMA will establish a cybersecurity (i.e., IA) personnel structure to implement the DCMA Cybersecurity (i.e., IA) Program. These personnel shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

2.8.1. Be the focal point for cybersecurity (i.e., IA) matters within DCMA.

2.8.2. Have the authority to enforce, with DAA concurrence, security policies and safeguards for DCMA systems and networks.

2.8.3. Recommend to the DAA suspension of system operations based on an identified security deficiency, poor security practice, or unacceptable risk.

2.8.4. Ensure operations do not negate system security.

2.9. INFORMATION SYSTEM OWNER (ISO). A Government ISO will be identified for each IS used by or in support of DCMA. If the ISO cannot be identified, then the IS should be deemed unnecessary and removed from the DCMA inventory. The ISO shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

2.9.1. Ensure the security of the IS as long as it remains in DCMA inventory, or until transferred (temporarily or permanently) to another Government person, organization, or agency; and such transfer is appropriately documented and provided as an artifact to the accreditation package.

2.9.2. Be responsible for the C&A of the IS and will provide the accreditation to the DCMA CA in sufficient time for review and determination of operational cybersecurity (i.e., IA) risk recommendation in support of DAA approval to operate decision prior to operational use or testing on a live network or with live DCMA data.

2.9.3. Plan and budget for IS certification efforts.

2.9.4. Not less than annually provide a written statement or digitally signed e-mail to the DCMA CA that either confirms the effectiveness of assigned cybersecurity (i.e., IA) controls and their implementation; recommends changes or improvements to the implementation of assigned cybersecurity (i.e., IA) controls; or assigns additional cybersecurity (i.e., IA) controls, changes, or improvements to the design of the IS itself.

2.10. DATA OWNER/INFORMATION OWNER. The data owner/information owner is the official with statutory or operational authority for specified information. The data owner shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

2.10.1. Establish controls for information generation, classification, collection, processing, dissemination, disposal, sensitivity, and need-to-know.

2.10.2. Assign the mission assurance category with the assistance of the C&A team.

2.11 CERTIFICATION AGENT (CA). The CA performs the functions for C&A and is a member of the C&A team. The CA shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall assist the ISO in the preparation system C&A packages and work to ensure that the security requirements are documented, tested, and implemented.

2.12. MANAGERS/SUPERVISORS. Managers/supervisors shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

2.12.1. Enforce users' suspensions and revocation for violations of access authorization.

2.12.2. Initiate access request for new users or access privilege changes.

2.13. GENERAL USER. Use of Government IS and access to Government networks is a revocable privilege, not a right. Users must have a favorable background investigation or hold a security clearance and access approvals commensurate with the level of information processed or available on the system. Users shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

- 2.13.1. Complete initial and/or annual cybersecurity (i.e., IA) training.
- 2.13.2. Maintain a degree of understanding of cybersecurity (i.e., IA) policies and doctrine commensurate with their responsibilities.
- 2.13.3. Adhere to the guidelines for DCMA automated ISs outlined in the DCMA authorized user agreement.
- 2.13.4. Be accountable for information assets assigned to them and protect those assets IAW applicable requirements.
- 2.13.5. Safeguard DCMA issued equipment.
- 2.13.6. Protect ISs and IS peripherals located in their respective areas IAW physical security and data protection requirements.
- 2.13.7. Comply with the Agency's acceptable use policy (AUP) for Government owned ISs and sign an AUP prior to or upon account activation.
- 2.13.8. Mark and safeguard files, output products, and storage media per the classification level and disseminate them only to individuals authorized to receive them with a valid need to know.
- 2.13.9. Protect ISs and IS peripherals located in their respective areas IAW physical security and data protection requirements. Apply additional safeguards and use a higher level or precaution to protect DCMA and DoD IS, IS peripherals, and information while traveling to foreign countries.
- 2.13.10. Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.
- 2.13.11. Obtain prior approval for the use of any media (for example, universal serial bus (USB), CD-ROM, floppy disk) from the local area network (LAN) administrator.
- 2.13.12. Scan all files, attachments, and media with an approved and installed anti-virus (AV) product before opening a file or attachment or introducing media into the IS.
- 2.13.13. Report all known or suspected spam, chain letters, and violations of acceptable use to the Network Operations and Security Center (NOSC).

2.13.14. Immediately stop using an infected IS and report suspicious, erratic, or anomalous IS operations; and missing or added files, services, or programs to the NOSC.

2.13.15. Not disclose their individual account password or pass-phrase authenticators.

2.13.16. Invoke password-protected screen when leaving workstation.

2.13.17. Logoff ISs at the end of each workday.

2.13.18. Access only that data, control information, software, hardware, and firmware for which the user is authorized access.

2.13.19. Access only that data that they are authorized or have a need to know.

2.13.20. Assume only authorized roles and privileges as assigned.

2.13.21. Users authorized Government-provided cybersecurity (i.e., IA) products (e.g., AV or personal firewalls) will be encouraged to install and update these products on their personal systems.

2.14. LEAD – IT ACCOUNTABLE PROPERTY OFFICER (APO). The Lead-IT APO shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

2.14.1. Report to the CIO an inventory of major ISs, including major national security systems, operated by or under the control of DCMA to include identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of DCMA.

2.14.2. Update inventory as changes occur. Inventory must be updated at least annually.

2.14.3. Maintain purchase record related to asset management.

2.14.4. Perform inventory management.

2.14.5. Ensure database of inventory is maintained and properly updated.

2.15. DCMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) COORDINATOR. The DCMA FISMA Coordinator shall abide by and support the responsibilities in Section 2.1 of this Instruction and shall:

2.15.1. Act as the PM and action officer to ensure that the data required for the regular and annual FISMA reports are completed in a timely manner to meet all Federal Information Security Management Act of 2002 (FISMA) section 3541 of Title 44, U.S.C. enacted as United States federal law Title III of the E-Government Act of 2002 requirements (Reference (z)).

2.15.2. Create Concept of Operations (CONOPs) and as needed, train the various accountable parties for the collection and submission of the required data for FISMA reporting.

2.15.3. Respond to and attend all FISMA related questions or events to ensure DCMA's requirements are heard and understood.

2.15.4. Be responsible for the development of and tracking of the processes associated with FISMA compliance, to include:

2.15.4.1. Creating metrics and reporting on those metrics monthly.

2.15.4.2. Ensuring any issues or problems that arise associated with reporting, FISMA processss, or the data received is elevated to the SISO and the CIO, as appropriate, in a timely manner.

2.15.4.3. Being responsible under MICP as the process owner for FISMA.

CHAPTER 3

PROCEDURES

3.1. CERTIFICATION AND ACCREDITATION (C&A)/RISK MANAGEMENT

FRAMEWORK (RMF). C&A is the foundational underlying process to execute the RMF and to ensure the DCMA IT systems have the minimal required security controls as per Chapter 1 of this Instruction. DCMA ISs shall be authorized to operate IAW DoDI 8510.01 (Reference (e)) and DODI 8500.01 (Reference (b)). The goal of C&A is to understand the vulnerabilities, determine the risk introduced through operations or connections of the system, and provide appropriate information for the DAA to consider the cybersecurity (i.e., IA) risk in contemplating an approval to operate decision. Statements of security requirements will be included in the earliest phases of the system acquisition, contracting, and development life cycles. Failure to implement proactive or corrective cybersecurity (i.e., IA) security measures, guidance, policy, or procedures may prevent system or enclave accreditation, installation, or operation and may increase system vulnerability to foreign and domestic computer network operation activities designed to deny service, compromise information, or permit unauthorized access to sensitive information. Cybersecurity (i.e., IA) or network personnel may block access to ISs that reflect poor cybersecurity (i.e., IA) security practices or fail to implement corrective measures.

NOTE: On March 12, 2014, DoD released DoDI 8510.01 (Reference (e)) establishing the RMF for DoD IT establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DIACAP and manages the life-cycle cybersecurity risk to DoD IT.

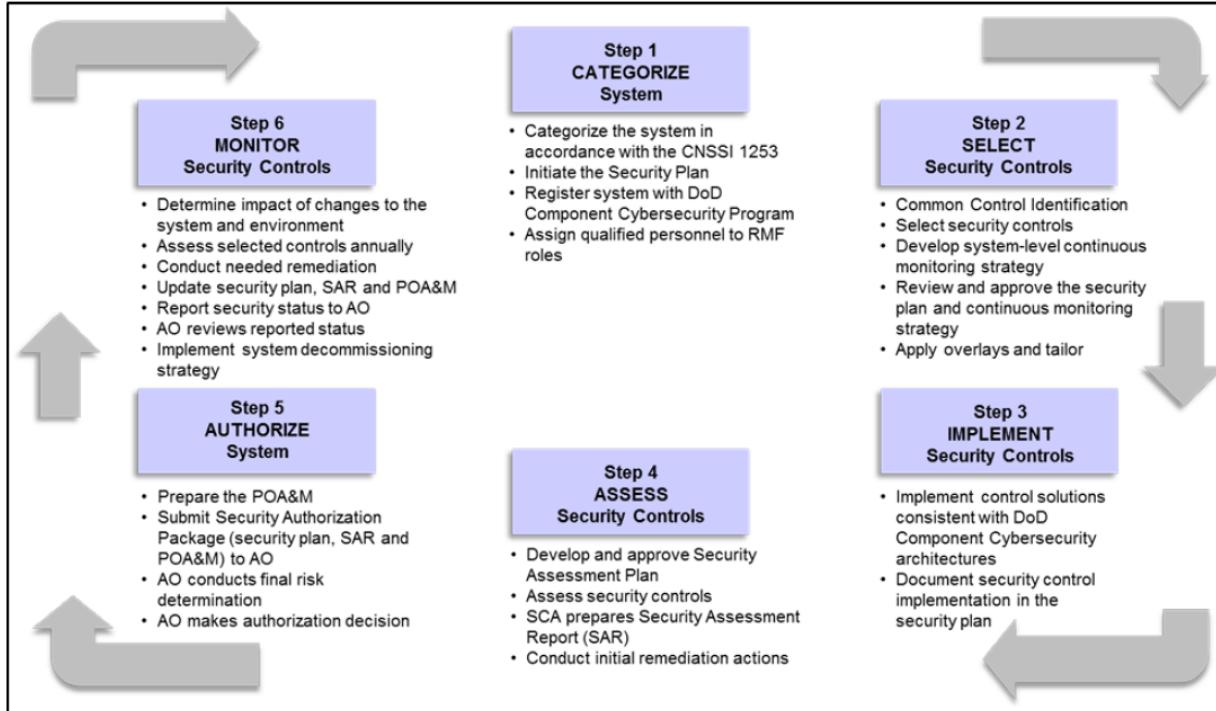
3.1.1. All DCMA ISs will be certified and accredited IAW the RMF for DoD IT. The DCMA implementation of RMF (see Figure 3) will document compliance detail of the NIST SP 800-53 (Reference (j)) security controls. The SISO will report the monthly status of the DCMA C&A to the CIO and will monitor the process for MICP.

3.1.2. Security Plan. DCMA IS and PIT systems must have a security plan that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The security plan should include implementation status, responsible entities, resources, and estimated completion dates. Security plans may also include, but are not limited to, a compiled list of system characteristics or qualities required for system registration, key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. The security plan is an integral part of the C&A/RMF process; templates will be provided by the C&A team.

3.1.3. Risk Management Framework (RMF) Steps. The RMF consists of the steps depicted in Figure 3. This process parallels the system life-cycle, with the RMF activities being initiated at the program or system inception (e.g., documented during capabilities identification or at the implementation of a major system modification). However, failure to initiate the RMF at system

or program inception is not a justification for ignoring or not complying with the RMF. The IS being accredited may be considered as a single system, system of systems, enclave or network.

Figure 3. Risk Management Framework



3.1.4. Mission Assurance Category (MAC). All ISs will be assigned a MAC that reflects the importance of the information relative to the achievement of DoD goals and objectives. The IS MAC will be determined by DoD or DCMA proponent and agreed upon by the DIACAP team. The MAC level is used to determine the cybersecurity (i.e., IA) controls for integrity and availability IAW DoDI 8500.01 (Reference (b)).

3.1.4.1. MAC I. MAC I is a high integrity, high availability for DoD ISs handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequence of loss of integrity or availability is unacceptable and could include the immediate and sustained loss of mission effectiveness.

3.1.4.2. MAC II. MAC II is a high integrity, medium availability for DoD ISs handling information that is important to the support of deployed and contingency forces. The consequence of loss of integrity is unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time.

3.1.4.3. MAC III. MAC III is a basic integrity, basic availability for DoD ISs handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences

of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness.

3.1.5. Confidentiality Levels. All ISs will be assigned a confidentiality level based on the classification or sensitivity of the information processed. The confidentiality level is used to establish acceptable access factors. DoD has defined the following three confidentiality levels:

3.1.5.1. Classified. Classified is information designated top secret, secret, or confidential IAW Executive Order 12356 “National Security Information” (Reference (aa)).

3.1.5.2. Sensitive. Information the loss, or unauthorized access to or modification of could adversely affect the national interest or conduct of Federal programs, or Privacy Act information. Includes, but is not limited to, for official use only (FOUO), CUI, privacy data, unclassified controlled nuclear information, and unclassified technical data.

3.1.5.3. Public. Information has been reviewed and approved for public release.

3.1.6. Certification. Cybersecurity (i.e., IA) certification considers:

3.1.6.1. The cybersecurity (i.e., IA) posture of the IS itself, that is the overall reliability and viability of the IS plus acceptability of the implementation and performance of cybersecurity (i.e., IA) mechanisms or safeguards that are inherent in the system itself.

3.1.6.2. How the system behaves in the larger information environment (for example, does it introduce vulnerabilities to the environment, does it correctly and securely interact with the information environment management and control services).

3.1.6.3. The certification determination based on actual results of the validation and the risk introduced by noncompliance with stated requirements.

3.1.6.4. Certification represents proof of compliance with this Instruction and DoDI 8500.01 (Reference (b)). Cybersecurity (i.e., IA) controls for the appropriate MAC level and the confidentiality level, at a minimum.

3.1.7. Accreditation. Accreditation is the official management ATO an IS or network.

3.1.8. Recertification and Reaccreditation. ISs will be recertified and reaccredited once every 3 years. Each of the cybersecurity (i.e., IA) controls assigned to the IS must be revalidated. The results of validation tests of cybersecurity (i.e., IA) controls conducted during an annual review may be used in the recertification and reaccreditation of the IS if performed within 1-year

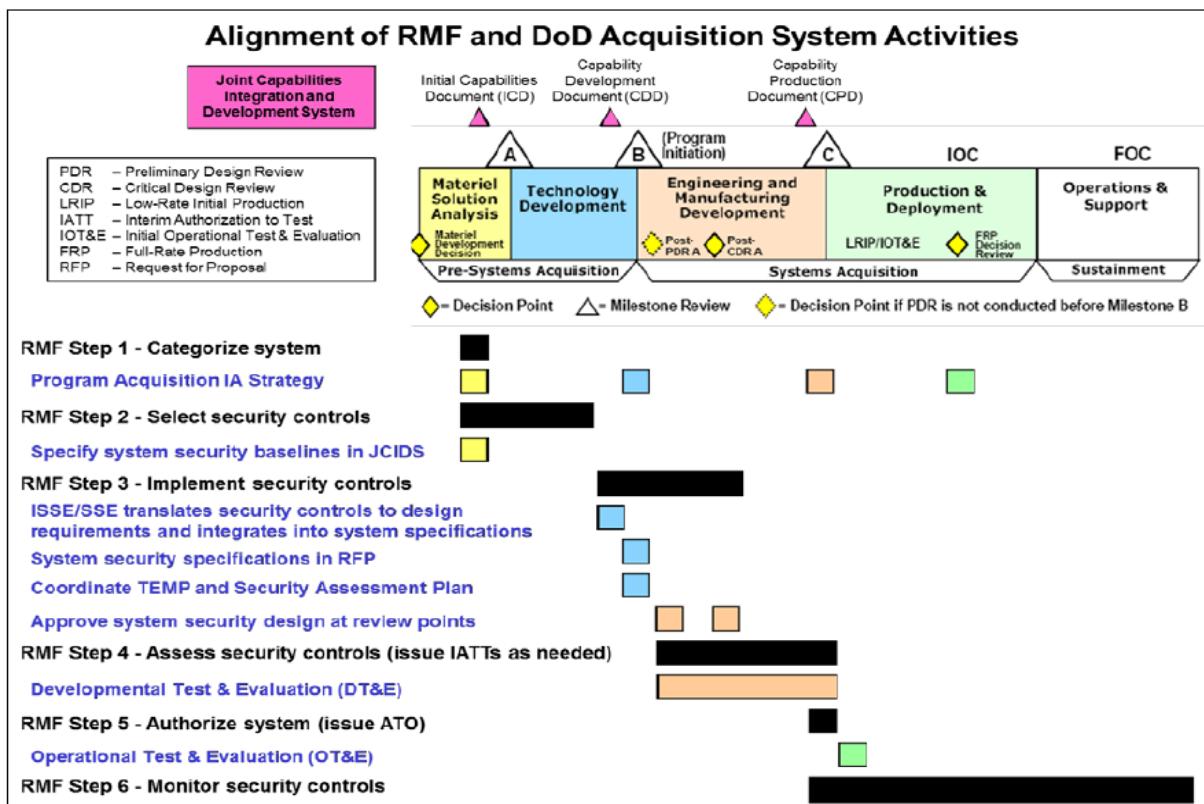
3.1.9. Monitoring Strategy. DCMA shall develop and document a system-level strategy IAW DoDI 8510.01 (Reference (e)) for the continuous monitoring of the effectiveness of security controls employed within or inherited by the system, and monitoring of any proposed or actual changes to the system and its environment of operation. The strategy must include the plan for annual assessments of a subset of implemented security controls, and the level of

July 10, 2014

independence required of the assessor. The breadth, depth, and rigor of these annual assessments should be reflective of the security categorization of the system and threats to the system. The CA should be integral to the development of this strategy. The system-level continuous monitoring strategy must conform to all applicable published DoD enterprise-level or DoD Component-level continuous monitoring strategies.

3.1.10. Integrating RMF into the Defense Acquisition Management System. The RMF is designed to be complementary to and supportive of DoD's acquisition management system activities, milestones, and phases. RMF activities should be initiated as early as possible in the DoD acquisition process to increase security and decrease cost. Requirements development, procurement, and RDT&E processes should be considered in applying the RMF to the acquisition of DoD IT. Threats to these systems should be designated consistent with the most severe risk to any individual component or subcomponent for consideration of requirements, acquisition, and testing and evaluation. Figure 4 illustrates the alignment of RMF steps to the acquisition life-cycle.

Figure 4. RMF and the DoD Acquisition Lifecycle



3.2. FISMA. The FISMA Act of 2002 requires federal agencies to develop, document, and implement an agency-wide cybersecurity program that includes periodic testing of the effectiveness of the management, operational, and technical controls of every IS identified in the inventory required under section 3505 of Title 44, U.S.C. (Reference (z)), to be performed with a frequency depending on risk, but no less than annually.

3.2.1. DCMA shall comply with the requirements FISMA Act of 2002 (Reference (z)), and enforce accountability for compliance with such requirements. DCMA will appoint a FISMA coordinator who will act as the PM for FISMA.

3.2.2. Annual Review. DCMA shall review annually the DCMA Cybersecurity (i.e., IA) Program and the coordinating cybersecurity policies, procedures, and cybersecurity programs.

NOTE: The RMF replaces the DIACAP and manages the life-cycle cybersecurity risk to DoD IT IAW DoDI 8510.01 (Reference (e)). In the near future, DCMA will phase out DIACAP and implement the RMF IAW guidance set forth in DoDI 8500.01 (Reference (b)).

3.3. COMPUTER NETWORK DEFENSE (CND). This mission area is focused on the prevention of damage to, protection of, investigation related to, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation, as defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (Reference (c)).

3.3.1. The DCMA NOSC Computer Network Defense Service Provider (CNDSP) provides Network Operations monitoring and CND services for the DCMA enterprise on both Non-secure Internet Protocol Router Network (NIPRNet) Unclassified and Secret Internet Protocol Router Network (SIPRNet) Classified operating environments to continuously protect, monitor, detect, analyze, and respond to unauthorized activity within DCMA and networks IAW DODI O-8530.2 (Reference (l)). This is achieved by providing the highest support possible in monitoring and maintaining continuous situational awareness of DCMA network performance and incidents on both unclassified and classified environments on a 7-day week, 24 hours a day, and 365 days a year.

3.3.2. DCMA employees role in CND/cybersecurity is that we all have a responsibility to **Protect Information**. All employees (civilian, military, and contractors) shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations. Refer to Chapter 2, Roles and Responsibilities, and section 3.4. DoD Information, of this Instruction for more details.

3.3.3. Monitoring Information Systems.

3.3.3.1. DCMA ISs (e.g., enclaves, applications, outsourced IT-based process, and PIT interconnections) shall be monitored to detect and react to incidents, intrusions, disruption of services, or other unauthorized activities, including insider threat, that threaten the security of DCMA operations or IT resources, including internal misuse.

3.3.3.2. DCMA employees will not use unapproved cybersecurity (i.e., IA) or IT tools. The DCMA Service Desk maintains an approved list of IA or IT tools and will provide guidance for use or procurement any required application. Use of these tools of this kind are limited to

certified technical staff members that work in DCMA-IT but there may be instances where users of DCMA IT systems may have access to or attempt to use cybersecurity (i.e., IA) tools in an attempt to troubleshoot IT system performance or connectivity. Any intentional misuse of tools to test, strain, or penetrate DCMA IT system or networks would constitute misuse of automated cybersecurity (i.e., IA) tools. Violations will be reported through appropriate command channels to the CIO and may result in disciplinary action, suspension of access privileges, and may be reportable as a security infraction to personnel security. If there are questions, contact the DCMA Service Center.

3.3.4. As a matter of normal auditing, DCMA cybersecurity (i.e., IA) or DCMA IT may review Web sites logs, files downloaded, ingress and egress services, and similar audited or related information exchanged over connected systems. Supervisors and managers may receive reports detailing the usage of these and other internal ISs, and are responsible for determining that such usage is both reasonable and authorized.

3.3.5. As a matter of normal auditing, DCMA cybersecurity (i.e., IA) or DCMA IT may store all files and messages through routine backups to tape, disk, or other storage media. This means that information stored or processed, even if a user has specifically deleted it, is often recoverable and may be examined at a later date by SA/NA and others permitted by lawful authority.

3.3.6. As required by Federal and DoD mandates, DCMA ISs shall be subjected to security penetration testing and other forms of testing used to complement monitoring activities consistent with DoDI 8560.01, “Communications Security (COMSEC) Monitoring and Information Assurance Readiness Testing” (Reference (ab)) and other applicable laws and regulations.

3.3.7. Incident and Intrusion Reporting. Incidents may result from accidental or deliberate actions on the part of a user or external influence. Time-sensitive actions are necessary to limit the amount of damage or access.

3.3.7.1. All DCMA personnel and DCMA IT account holders will protect IS incident reports as a minimum FOUO or to the level for which the system is accredited or as directed by system classification guide.

3.3.7.2. An individual who suspects or observes an unusual or obvious incident or occurrence will immediately notify the DCMA NOSC. All personnel will report IS incidents or events including, but not limited to:

- Known or suspected intrusion or access by an unauthorized individual
- Authorized user attempting to circumvent security procedures or elevate access privileges
- Unexplained modifications of files, software, or programs
- Unexplained or erratic IS system responses
- Presence of suspicious files, shortcuts, or programs
- Malicious logic infection (e.g., virus, worm, Trojan)

- Receipt of suspicious e-mail attachments, files, or links
- Spillage incidents
- Adverse effects on the DCMA's image such as Web page defacements
- Access or compromise of classified, sensitive, or protected information (e.g., social security number, soldier identification information, medical condition or status, doctor-patient, or attorney-client privilege)
- Compromise originating from a foreign source
- Compromise of systems that may risk safety, life, limb, or has the potential for catastrophic effects, or contain information for which the DCMA is attributable
- Loss of any IS or media containing protected or classified information

3.4. DOD INFORMATION.

3.4.1. Information Security (INFOSEC). The DCMA Information Security Program is described in DCMA-INST 552 (Reference (y)). All classified information and CUI must be protected IAW references DoDM 5200.01, Volume 1 (Reference (t)); DoDM 5200.01, Volume 2 (Reference (v)); DoDM 5200.01, Volume 3 (Reference (m)); DoDI 5200.01 “DoD Information Security Program and Protection of Sensitive Compartmented Information” (Reference (ac)); and DoDM 5200.01, Volume 4 (Reference (n)).

3.4.1.1. ISs must protect classified information and CUI from unauthorized access by requiring authentication IAW DoDI 8520.03 “Identity Authentication for Information Systems” (Reference (ad)) prior to making an access decision.

3.4.1.2. Security Incidents. Protection of classified information and CUI is essential to maintaining security and achieving mission success in DoD’s operational environments. Prompt reporting of actual or suspected security incidents ensures that incidents are properly investigated and necessary actions are taken to negate or minimize the adverse effects of an actual loss or unauthorized disclosure of classified information. Handling of security incidents are addressed in Chapter 9 of DCMA-INST 552 (Reference (y)).

3.4.1.3. All information presented publicly must comply with guidance established by DCMA-INST 522, “Public Affairs” (Reference(ae)). (This includes information posted to public facing Web sites, Facebook, Blogs, etc.). All unclassified DoD information that has not been cleared for public release IAW DoDD 5230.09, “Clearance of DoD Information for Public Release” (Reference (af)) and that is in the possession or control of non-DoD entities on non-DoD ISs, must be protected IAW DoDI 8582.01, “Security of Unclassified DoD Information on Non-DoD Information Systems” (Reference (ag)).

3.4.1.4. DoD IT that processes or stores PII or protected health information must comply with DoD Regulation 5400.11-R, “Department of Defense Privacy Program (Reference (ah)); DoDI 5400.16, “DoD Privacy Impact Assessment (PIA) Guidance” (Reference (ai)); and DoD Regulation 8580.02-R, “DoD Health Information Security Regulation” (Reference (aj)).

3.4.2. Operational Security (OPSEC). DCMA stores, processes, and transmits critical information, sensitive Scientific and Technical Information, Military Critical Technologies List,

International Traffic-in-Arms Regulations (ITAR), and Export Control Law restricted information, as well as Freedom of Information Act (FOIA)-exempted information on DCMA IS. OPSEC must be considered before posting information in a shared environment or on publicly available Web pages. DCMA's OPSEC program is outlined within DCMA-INST 556, "Operation Security" (Reference (ak)).

3.4.2.1. DCMA personnel should remain vigilant and only discuss or provide access to DCMA information when a valid need-to-know is established.

3.4.3. Physical Security. DCMA personnel are required to protect IT resources from damage, loss, theft, or unauthorized physical access IAW DCMA-INS 557, "Physical Security," (Reference (al)) and DoD Regulation 5200.08-R (Reference (t)).

3.4.3.1. Clearances. Personnel will be cleared to the highest level of data handled by the IS.

3.4.3.2. Restrictions. An escort is required for personnel not meeting required clearance level at all times by a cleared and technically qualified individual.

3.4.4. Information Access. Access control is the process of granting or denying requests to DoD information or ISs. Access to DCMA ISs is a revocable privilege and shall be granted to individuals based on need-to-know and IAW DCMA-INST 806, "Networks and Application Access" (Reference (am)); DODI 8510.01 (Reference (e)); NSTISSP No. 200, "National Policy on Controlled Access Protection" (Reference (ao)); Status of Forces Agreements (SOFA) for host national access, and DoD Regulation 5200.2-R (Reference (s)).

3.4.4.1. Requirements for DCMA IS Access. All IS access requests must follow guidance set forth in DCMA-INST 806 (Reference (am)) to include proper cybersecurity (i.e., IA) training, agree to and signed AUP, and personnel security standards.

3.4.4.1.1. Security Awareness Training. All DCMA employees and IS users shall maintain a degree of understanding of cybersecurity (i.e., IA) policies and doctrine commensurate with their responsibilities. They shall be capable of appropriately responding to and reporting suspicious activities and conditions, and they shall know how to protect the information and IS they access. To achieve this understanding, all DCMA employees and IS users of DCMA systems or networks shall receive both initial and periodic refresher cybersecurity (i.e., IA) training. All users must receive cybersecurity (i.e., IA) awareness training tailored to the system and information accessible before issuance of a password for network access. The training will include the following:

- Threats, vulnerabilities, and risks associated with the system. This portion will include specific information regarding measures to reduce malicious logic threats, principles of shared risk, external and internal threat concerns, acceptable use, privacy issues, prohibitions on loading unauthorized software or hardware devices, and the requirement for frequent backups
 - Information security objectives (i.e., what needs to be protected)
 - Responsibilities and accountability associated with cybersecurity (i.e., IA)

- Information accessibility, handling, and storage considerations
- Physical and environmental considerations necessary to protect the system
- System data and access controls
- Incident, intrusion, malicious logic, virus, abnormal program, or system response reporting requirements
 - Information operations condition (INFOCON) requirements and definitions
 - AUP requirements

3.4.4.1.2. DCMA provides basic security awareness training to IS users (including managers, senior executives, and contractors):

- As a part of initial training for new users
- When required by IS changes
- As an annual refresher training as a minimum or as conditions warrant
- Provided with the issuance of a SIPRnet account

3.4.4.2. Acceptable Use Policy (AUP). The DCMA AUP outlines terms and conditions for use of DCMA ISs. All DCMA users will review and sign an AUP prior to or upon account activation. Digital signatures are authorized. The following items are included in the DCMA AUP:

3.4.4.2.1. DOD policy states that Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, internet systems, and commercial systems), when use of such systems and equipment is paid for by the Federal Government, will be for official use and authorized purposes only. Official use includes emergency communications and communications necessary to carry out the business of the Federal Government. Official use can also include other use authorized by a theater commander for Soldiers and civilian employees deployed for extended periods away from home on official business. Authorized purposes include brief communications by employees while they are traveling on Government business to notify family members of official transportation or schedule changes. Authorized purposes can also include limited personal use established by appropriate authorities under the guidelines of the DoD Regulation 5500.7-R, “Joint Ethics Regulation” (Reference (ao)).

3.4.4.2.2. Certain activities are never authorized on DCMA networks. AUPs will include the following minimums as prohibited. These activities include:

3.4.4.2.2.1. Use of ISs for unlawful or unauthorized activities such as file sharing of media, data, or other content that is protected by Federal or state law, including copyright or other intellectual property statutes.

3.4.4.2.2.2. Modification of the IS or software, use of it in any manner other than its intended purpose, or adding user-configurable or unauthorized software such as, but not limited to, commercial instant messaging, commercial Internet chat, collaborative environments, or peer-to-peer client applications. These applications create exploitable vulnerabilities and circumvent normal means of securing and monitoring network activity and provide a vector for

the introduction of malicious code, remote access (RA), network intrusions, or the exfiltration of protected data.

3.4.4.2.2.3. Attempts to strain, test, circumvent, or bypass network or IS security mechanisms, or to perform network or keystroke monitoring. CNDSP, Red Team, or other official activities, operating in their official capacities only, may be exempted from this requirement.

3.4.4.2.2.4. Physical relocation or changes to configuration or network connectivity of IS equipment.

3.4.4.2.2.5. Installation of non-Government-owned computing systems or devices without prior authorization of the appointed DAA including but not limited to USB devices, external media, personal or contractor-owned laptops.

3.4.4.2.2.6. Release, disclose, transfer, possess, or alter information without the consent of the data owner, the original classification authority as defined by DCMA-INST 552 (Reference (y)), the individual's supervisory chain of command, FOIA official, Public Affairs Office, or disclosure officer's approval.

3.4.4.2.2.7. Sharing personal accounts and authenticators (passwords or personal identification numbers (PIN)) or permitting the use of RA capabilities through Government-provided resources with any unauthorized individual.

3.4.4.2.2.8. Disabling or removing security or protective software and other mechanisms and their associated logs from IS.

3.4.4.3. IT Position Categories. The following standards designate positions requiring access to IT for processing information within IT systems. The security designations are required to distinguish potential adverse effects on DCMA functions and operations and, therefore, the relative sensitivity of functions performed by individuals having certain privileges. These positions are referred to as IT and IT-related positions. The requirements of this section will be applied to all IT and IT-related positions, whether occupied by civilians, military personnel, consultants, contractor personnel, or others affiliated with the DoD. Position categories include: IT-I (Privileged), IT-II (Limited Privileged), and IT-III (Non-Privileged). Additional guidance is available in DCMA-INST 555, "Personnel Security" (Reference (ap)) and DoD Regulation 5200.2-R (Reference (s)). Table 1 and Table 2, at the end of this section summarize investigative level requirements for access.

3.4.4.3.1. Personnel Security Controls.

3.4.4.3.1.1. Position categories are assigned a position designation using the criteria found in DoD Regulation 5200.08-R (Reference (u)) and DoDI 1400.25 Volume 731, "DoD Civilian Personnel Management System: Suitability and Fitness Adjudication For Civilian Employees" (Reference (aq)). The position designation will be documented in the Defense Civilian Personnel Data System (DCPDS). **NOTE:** IT-I, IT-II, or IT-III are used in lieu of Automated Data Processing (ADP) levels (i.e., ADP-I, ADP-II, and ADP-III).

3.4.4.3.1.1. Individuals assigned to IT-I, IT-II, or IT-III positions who lose their clearance, or have access to classified systems suspended pending the results of an investigation, will be barred access to the ISs until favorable adjudication of that investigation. Waivers for continued access to unclassified systems will be justified in a written request, with the Director's concurrence, to the DAA for approval. Access will be granted only upon DAA authorization. This request and approval will become part of the C&A package. Users designated in IT-I positions will be removed from these positions and this denial of access is non-waiverable.

3.4.4.3.1.2. Waivers processed for IT-II and IT-III personnel only are valid for a period not to exceed 6 months. If a second waiver extension is required, one may be granted as long as a new request for waiver is submitted to the DAA and approved by the first general officer, or equivalent in position or civilian grade, in the chain of command.

3.4.4.3.1.3. Contractor, foreign national (FN), or temporary individuals assigned to any IT positions who have their unclassified system or network accesses revoked or suspended for derogatory reasons, will be barred access to the ISs until favorable adjudication of that investigation.

3.4.4.3.1.4. Reinvestigation. Individuals occupying an IT position will be subject to a periodic reinvestigation according to DCMA personnel security policy.

Table 1. Investigative Levels for User with IA Management Access to DoD Unclassified Systems

Investigative Levels for User with IA Management Access to DoD Unclassified Systems					
(Investigative levels are defined in DoD Regulation 5200.2-R)					
-- The term foreign nationals (FN) refers to all individuals who are Non-U.S. citizens including U.S. military personnel, DoD civilian employees, and contractors --					
User Roles	FN (See Note)	U.S. Civilian	U.S. Military	U.S. Contractor	Conditions or Examples
IAM (with no IA administrative privileges)	Not Allowed	NACI	NACLC	NACLC	None
IAO (with no IA administrative privileges)	Conditional Allowed – NACLC – (equivalent)	NACI	NACLC	NACLC	FN - With DAA written approval, direct or indirect hires may continue as IAOs until replaced, provided they serve under immediate supervision of a U.S. citizen IAM, and have no supervisory duties.
Supervisor of IT-II or IT-I positions	Not Allowed	NACI	NACLC	NACLC	None
Administrator (with no IA administrative privileges)	Allowed: NACLC – (equivalent)	NACI	NACLC	NACLC	Examples: AIS, OS, or end-user administration, administration of applications (e.g., e-mail, word) FN - Under immediate supervision of a U.S. citizen.
Maintenance of IA-enabled products	Conditional Allowed – NACLC – (equivalent)	NACI	NACLC	NACLC	FN - Under the immediate supervision of a U.S. citizen with technical understanding of tool / products maintained.
DAA or IAM	Not Allowed	SSBI	SSBI	SSBI	None

Table 1. (continued) Investigative Levels for User with IA Management Access to DoD Unclassified Systems

User Roles	FN (See Note)	U.S. Civilian	U.S. Military	U.S. Contractor	Conditions or Examples
IAO (with IA administrative privileges)	Conditionally Allowed – SSBI – (equivalent)	SSBI	SSBI	SSBI	FN - With DAA written approval, direct or indirect hires may continue as IAOs until replaced, provided they serve under the immediate supervision of a U.S. citizen IAM, and have no supervisory duties.
Monitoring and testing	Not Allowed	SSBI	SSBI	SSBI	None
Administrator (with IA administrative privileges)	Conditionally Allowed – SSBI – (equivalent)	SSBI	SSBI	SSBI	Examples: Administration of IA devices (e.g., boundary devices, IDS, routers and switches) FN - Under the immediate supervision of a U.S. citizen, and with written approval of the Head of the DoD Component
Maintenance of IA products	Conditionally Allowed - SSBI - (equivalent)	SSBI	SSBI	SSBI	FN - Under the immediate supervision of a U.S. citizen technical understanding of tool / products maintained, and with written approval of the Head of the DoD Component All - Also subject to IA controls

Note: FN direct and indirect hires covered by the provisions of a Status of Forces Agreement (SOFA), or other international agreement, require host-nation personnel security investigations that are the equivalent of the U.S. investigative level indicated.

Table 2. Investigative Levels for DoD Information System Users Responsible for PKI Certificate Issuance

Investigative Levels for DoD Information System Users Responsible for PKI Certificate Issuance				
User Roles	Foreign National	U.S. Civilian	U.S. Military	U.S. Contractor
Unclassified and Classified (SECRET and Below) Certificate Issuance - (IT-II)	Not Allowed	NACI	NACLC	NACLC
Classified Certificate Issuance - ABOVE SECRET - (IT-I)	Not Allowed	SSBI	SSBI	SSBI

3.5. CYBERSECURITY WORKFORCE.

3.5.1. Cybersecurity (i.e., IA) Workforce Training. IAW DoDI 8570.01 (Reference (k)) and DoD 8570.01-M (Reference (x)), all DCMAIT personnel (i.e., military or civilian) or DCMAIT-assigned support contractor personnel having cybersecurity (i.e., IA) as a primary duty, or having elevated network privileges, will:

- Be designated as such in writing
- Be trained to a minimum standard commensurate with their duties and responsibilities
- Receive certification from a recognized credentialing authority
- Maintain their certification status

3.5.2. All cybersecurity personnel must be assigned in writing to identified cybersecurity positions, and trained and qualified IAW DoDD 8570.01 (Reference (k)) and DoD 8570.01-M (Reference (x)).

3.6. MISSION PARTNERS. Mission partners are those whom the Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector. Integral to the success of the Defense cybersecurity program is the promotion of systems and communications interoperability and advancement of operational cybersecurity and cyberspace defense relationships with all mission partners at both the unclassified and classified levels; integration of cybersecurity and cyberspace defense activities with mission partner critical infrastructure protection initiatives; and creating cybersecurity and cyberspace defense training and exercise opportunities to build mission partner operational capacity, improve global cyber situational awareness, and develop a collective global cybersecurity and cyberspace defense workforce. This will be accomplished through the planning, negotiation, and implementation of cybersecurity and cyberspace defense agreements with mission partners.

3.6.1. Authorized users who are contractors as described in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F “Information Assurance (IA) and Support to Computer Network Defense (CND)” (Reference (ar)), shall always have their contractor affiliation displayed as “CTR” as part of their e-mail addresses.

3.6.2. FNs represent a unique challenge for the Agency because DCMA relies on the provisions of a SOFA, or other international agreement, requirement of host-nation personnel security investigations that are stated to be the equivalent of the U.S. investigative level indicated. Each host country performs the security investigations different and the adjudicator of the clearance is not standardize IAW Executive Order 12968, “Access to Classified Information” (Reference (as)) and DoD 5200.2- R (Reference (s)). Foreign exchange personnel and representatives of foreign nations, coalitions, or international organizations may be authorized access to DoD ISs containing classified or sensitive information only if these conditions are met:

3.6.2.1. Access to DoD ISs is authorized only by the DoD Component head IAW DoD, Department of State, and Office of the Director of National Intelligence disclosure guidance, as applicable. For DCMA this means all requests for access to a DCMA IT system will be reviewed on a case-by-case basis. All requests for access will be staffed via a memorandum for record (MFR) signed by the first Senior Executive Service (SES) or flag officer in the chain of command and routed through the DCMA CIO to the DCMA Deputy Director. As part of the process for approval, the DCMA CIO will contact Directorate for Security and Safety for review, auditing, and approval prior to making a risk based recommendation to the Deputy Director.

3.6.2.2. DCMA shall create mechanisms to limit access strictly to information that has been cleared for release to the represented foreign nation, coalition, or international organization (e.g., North Atlantic Treaty Organization) IAW DODI 2030.08, “Implementation of Trade Security Controls (TSC) and Commerce Control List (CCL) Personal Property to Parties Outside DoD Control” (Reference (at)) for classified military information, and other policy guidance for unclassified information such as DoDM 5200.01 Volume 4 (References (n)), DoDI 1400.25 Volume 731 (Reference (aq)), DoDD 5230.20, “Visits and Assignments of Foreign Nationals” (Reference (au)), and DoDI 5230.27, “Presentation of DoD-Related Scientific and Technical Papers at Meetings” (Reference (av)). If DCMA does not have the capability to limit access due to IT design or architectural limitations, then this shall weigh heavily and be highlighted as a factor of the risk based decisions for allowing FN access to DCMA IT systems or DCMA electronic data.

3.6.2.3. Access to DCMA-owned and DCMA-managed ISs with CUI will be on a need-to-know basis for official duties by FNs (e.g., DoD FN employees (direct or indirect hires)) or military, civilian, or contract employees of foreign governments serving with DCMA. As part of the request for foreign access to DCMA IT system or electronic data labelled or classified as CUI, the MFR shall state the specific need-to-know requirements for the FN to obtain access to that data and or IT system.

3.6.2.4. Prior to authorizing FN access to specific ISs, all access requirements set forth in CJCSI 6510.01 Enclosure C Section 27 (Reference (ar)) must be satisfied.

3.6.2.5. If the DCMA Director, or designee, authorizes the FNs (DoD direct or indirect hire FN employees or foreign representatives as described CJCSI 6510.01F (Reference (ar))) to have access to the DCMA network or specific IT systems, they shall always have their country affiliation displayed as part of their e-mail addresses.

3.6.2.6. FNs are not authorized access or be in the same physical space where any classified data or systems that are Secret or higher classification is processed.

3.6.3. Capabilities built to support cybersecurity objectives that are shared with mission partners will be governed through integrated decision structures and processes described in this Instruction, must have formal agreements (e.g., a memorandum of agreement, memorandum of understanding, service level agreements, contracts, grants, or other legal agreements or understandings) that incorporate considerations for DoD risks, be IAW CJCSI 6211.02, “Defense Information System Network (DISN) Responsibilities” (Reference (aw)), and will be consistent with applicable guidance contained in DoDD 5230.11, “Disclosure of Classified Military Information to Foreign Governments and International Organizations” (References (ax)); DoD Manual 5200.01 Volume 3 (Reference (m)); DoDM 5200.01 Volume 4 (Reference (n)); Title 29 U.S.C. (Reference (q)); DoD Manual 5200.01 Volume 1 (Reference (t)); DoDM 5200.01 Volume 2 (Reference (v)); and DoDI 2040.02, “International Transfers of Technology, Articles, and Services” (Reference (ay)).

3.6.4. ISs jointly developed by DoD and mission partners are considered DoD-partnered systems. The cybersecurity risk management considerations for DoD-partnered systems are provided in Reference (e).

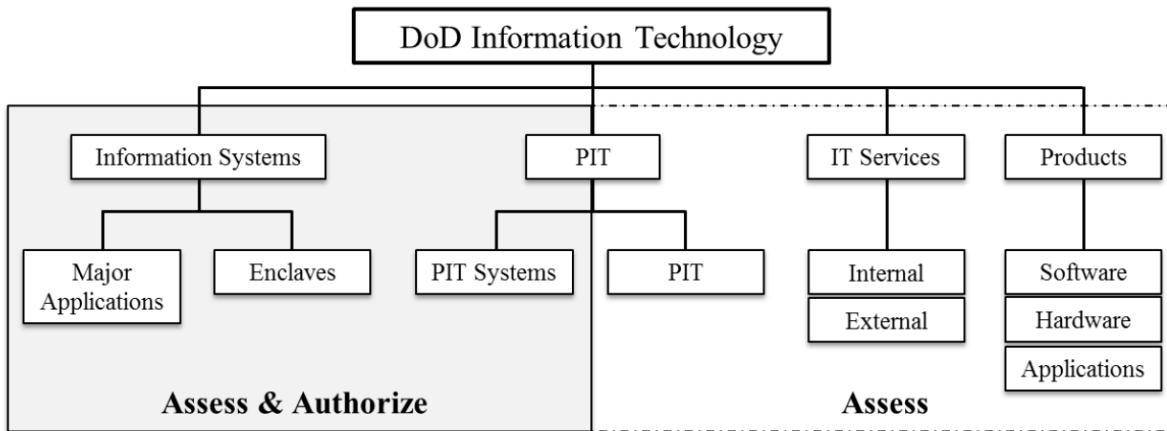
3.6.5. Agreements with international partners to engage in cooperative international cybersecurity activities must be formally negotiated and concluded IAW DoDD 5530.3, “International Agreements” (Reference (az)), and any associated classified military information will be released only IAW DoDD 5230.11 (Reference (ax)).

3.6.6. The release of cryptographic national security systems technical security material, information, and techniques to foreign governments or international organizations must be approved by the Committee on National Security Systems (CNSS) IAW National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems” (Reference (ba)).

3.6.7. Due to the sensitivity of the information that DCMA handles on its IS, contractors, foreign persons, and other mission partners should be required to sign a Non-Disclosure Agreement restricting the sharing of information gained while accessing a DCMA IS.

3.7. INFORMATION TECHNOLOGY (IT). Cybersecurity (i.e., IA) applies to all IT that receives, processes, stores, displays, or transmits DoD information, as shown in Figure 5.

Figure 5. DoD Information Technology



3.7.1. Information Systems (IS). Cybersecurity (i.e., IA) requirements must be identified and included in the design, development, acquisition, installation, operation, upgrade, or replacement of all DCMA ISs IAW section 35 of Title 44 (Reference (f)); DoDI 8510.01 (References (e)); DoDD 8000.01, “Management of the Department of Defense Information Enterprise” (Reference (bb)); section 2224 of Title 10, U.S.C. (Reference (bc); this Instruction; and other cybersecurity-related DoD guidance, as issued.

3.7.1.1. DoD ISs are typically organized in one of two forms:

3.7.1.1.1. Enclave. Enclaves provide standard cybersecurity, such as boundary defense, incident detection and response, and key management, as well as, deliver common applications, such as office automation and electronic mail. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include LANs and the applications they host, backbone networks, and data processing centers. Enclaves always assume the highest security category of the ISs that they host, and derive their security needs from those systems.

3.7.1.1.2. Major Application. Certain applications, because of the information in them, require special management oversight due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application and should be treated as major applications. A major application may be a single software application (e.g., integrated consumable items support), multiple software applications that are related to a single mission (e.g., payroll or personnel), or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Enrollment Eligibility Reporting System). All software/applications, regardless of whether they rise to the level of major application or not, require an appropriate level of protection. Adequate security for other than major applications may be provided by security of the environment in which they operate. Additional guidance is set forth to ensure application security within DoDI 8500.01 (Reference (b)).

3.7.1.2. Notice and Consent Banners. Standard mandatory notice and consent banners must be displayed at logon to all ISs.

3.7.2. IT Products.

3.7.2.1. All DCMA IT products must comply with applicable security technical implementation guides (STIG), security configuration guides, and security requirements guide with any exceptions documented and approved by the responsible AO.

3.7.2.2. Software.

3.7.2.2.1. All software installed on DCMA ISs must be approved prior to install. Approved software is listed on the DCMA Approved Software list available on the DCMA IT 360 site. Software listed on the DCMA Unauthorized software list is prohibited. Any new software product must go through the systems change request (SCR) process to be approved for installation. The SCR process is outlined within DCMA-INST 810, “DCMA IT Acquisitions - Non-Programmed Acquisitions Valued At \$3,000 Or Below” (Reference (bd)). Once a product is approved, it will be added to the DCMA Approved Software list.

3.7.2.2.2. All commercial off-the-shelf (COTS) software used on DCMA ISs will be fully licensed (under U.S. Copyright Law).

3.7.2.2.3. Use of shareware or freeware is prohibited unless specifically approved through the DCMA SCR process and listed on the DCMA Approved software list.

3.7.2.2.4. Automated Updates. DCMA ISs must maintain up-to-date software patches and AV software definitions. Patches are applied to all DCMA ISs on a regular basis by automated processes. Any system that does not update via the DCMA automated process will require manual application of vulnerability patches and AV signatures. All DCMA ISs must maintain AV signatures within 30 days. Any computer with AV signature definitions exceeding 30 days will be disconnected from the network until all files are updated.

3.7.2.2.5. Peer-to-Peer (P2P). P2P file sharing is an IT that permits computer users to share files with other users. The installation and use of unauthorized P2P file sharing applications can result in significant vulnerabilities to DoD and DCMA ISs. P2P is prohibited on DCMA ISs.

3.7.2.2.6. Out-of-the-box configurations of COTS purchased products is prohibited. COTS purchased products will require SCR Approval, C&A authorization, STIG, and IA (i.e., cybersecurity) vulnerability management (IAVM) compliance as a minimum. Comprehensive vulnerability assessments of the test IS will be conducted and documented before and after installation of any COTS products under consideration for SCR review or approval.

3.7.2.2.7. Database Integrity. Databases store information and will be managed to ensure that data is accurate, protected, accessible, and verifiable so that commanders at all levels can rely on trusted information in the decision making process. Database security must:

3.7.2.2.7.1. Be STIG compliant.

3.7.2.2.7.2. Implement safeguards to detect and minimize unauthorized access and inadvertent, malicious, or non-malicious modification or destruction of data.

3.7.2.2.7.3. Implement safeguards to ensure that security classification levels remain with the transmitted data.

3.7.2.2.7.4. Use data or data sources that have verifiable or trusted information. Examples of trusted sources include, but are not limited to, information published on DoD and DCMA sites and vendor sites that use verified source code or cryptographic hash values.

3.7.2.2.7.5. Protect data at rest (for example, databases, files) to the classification level of the information with authorized encryption and strict access control measures implemented.

3.7.2.2.8. Mobile Code. Mobile code is executable software, transferred across a network, downloaded, and executed on a local system without notification to, or explicit installation and execution by, the recipient. Mobile code has the potential to severely degrade operations if improperly used or controlled. DCMA shall deny untrusted mobile code the ability to traverse the DCMA enterprise. Mobile code technologies (e.g., Java Virtual Machine, Java compiler, .Net Common Language Runtime, Windows Scripting Host, and Hypertext Markup Language (HTML) Application Host) shall be categorized, evaluated, and controlled to reduce the risk to DCMA ISs.

3.7.2.3. Hardware. An SCR submittal and approval is required prior to modifying or reconfiguring the hardware of any computer system. Hardware will not be connected to any system or network without SCR approval.

3.7.2.4. Portable Electronic Devices (PED) and Removable Media. Government-owned PEDs (e.g., laptop computers, personal digital assistants (PDA), blackberry devices, and cell phones) including removable media (e.g., diskettes, compact disks (CD), and external hard drives) shall be properly accounted for, properly marked, properly transported, and secured at all times to the highest level of classified information processed. PEDs, including removable media, shall be secured with approved security applications and data-at-rest solutions IAW DoD CIO memorandum, “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media” (Reference (be)).

3.7.3. IT Considerations. These are general considerations that apply to IT.

3.7.3.1. Remote Access (RA)/Telework. RA/telework is a critical part of the DCMA IT Services offered to the Agency due to the geographically dispersed and mobile workforce. DoD has increased the security constraints related to RA to DoD IT systems and data due to the current and forecasted threat environment.

3.7.3.1.1. DCMA shall comply with the provisions of DoDI 1035.01, “Telework Policy” (Reference(bf)):

3.7.3.1.1.1. Telework solutions involving the use of DoD-owned, government-furnished equipment for RA to unclassified DoD networks will comply with the requirements of applicable security controls defined in NIST 800-53 (Reference (j)).

3.7.3.1.1.2. Telework solutions involving the use of non-government furnished equipment (GFE) (i.e., any computer or other telework device not furnished by DoD) for RA to unclassified DoD networks will be developed by the DoD Components (DCMA) desiring the capability based on the guidance provided in NIST SP 800-114, “Users Guide to Securing External Devices for Telework and Remote Access” (Reference(bg)) and evaluated and approved by the DoD CIO on a case-by-case basis. DCMA currently does not have any approved non-GFE solution approved by the DoD CIO. This requirement is from DoDI 8500.01 (Reference (b)). DCMA IT will work with the DoD CIO to make our solutions meet the regulation stipulation or remove this capability from our inventory.

3.7.3.1.2. In addition to paragraph 3.7.3.1.1., DCMA Systems being used for RA/telework RA shall:

3.7.3.1.2.1. Meet security configurations to include IAVM, C&A standards, and will employ host-based security; for example, a firewall and intrusion detection system (IDS), with AV software before authorization to connect to any RA server. Security configurations will be reviewed quarterly.

3.7.3.1.2.2. Encrypt log-in credentials as they traverse the network as required for the level of information being accessed or required for need-to-know separation.

3.7.3.1.2.3. Encrypt all RA for network configuration or management activities regardless of classification level, device, or access method.

3.7.3.1.2.4. Users will protect RA ISs and data consistent with the level of information retrieved during the session. Any information posted for general DCMA consumption should not contain CUI information

3.7.3.1.2.5. Disable remote device password save-functions incorporated within software or applications to prevent storage of plain text passwords.

3.7.3.1.2.6. RA users will read and sign security and end-user agreements for RA annually as a condition for continued access.

3.7.3.1.2.7. Users will protect RA/telework ISs and data consistent with the level of information retrieved during the session.

3.7.3.1.2.8. Users will implement additional safeguards and use extra precautions to protect RA/telework ISs and data when traveling internationally.

3.7.3.1.2. FNs will not be permitted to telework. Waivers for FN employees will only be authorized by the Director of DCMA International, or designee. For DCMA this means all requests for FNs to telework will be reviewed on a case-by-case basis. All requests will be staffed via a MFR, signed by the first SES or flag officer in the chain of command and through the Director of DCMA International. Once approved, as part of the process, the DCMA CIO will receive the signed MFR and contact Directorate for Security and Safety for review, documenting the risk.

3.7.3.2. Web Site Security.

3.7.3.2.1. Access to DCMA-owned, -operated or -outsourced Web sites shall be strictly controlled by the Web site owner using technical, operational, and procedural measures appropriate to the Web site audience and information classification or sensitivity.

3.7.3.2.2. Access to DCMA-owned, -operated or -controlled Web sites containing official information shall be granted according to DCMA-INST 806 (Reference (am)) and need-to-know rules established by the information owner.

3.7.3.2.3. Access to DCMA-owned, -operated or -controlled Web sites containing public information is not restricted; however, the information accessible through the Web sites shall be limited to unclassified information that has been reviewed and approved for release IAW DoDD 5230.09 (Reference (af)) and DoDI 5230.29, “Security and Policy Review of DoD Information for Public Release” (References (bh)).

3.7.3.3. Reuse of DCMA Hard Drives (HDD). The following provides the process for the reuse of HDDs used to handle DCMA information. This process will be used when:

- Drives will be re-purposed to a different environment than the one in which they were previously used (new users without a need-to-know for the original data) or to
- Process data at a different classification or sensitivity level
- Drives have met their scheduled end of their lifecycles
- Drives have failed

3.7.3.3.1. Destruction or removal of information on DCMA hardware HDDs will only be performed through the use of approved methods.

3.7.3.3.2. IS will not be released for reuse until they have been:

- Checked for presence of installed drives
- Externally labeled with a verification of the number of drives installed/removed
- Certified that all drives have been purged.

3.7.3.3.3. IAW this Instruction, DCMA hardware, to include HDDs, will be accounted for.

3.7.3.3.4. HDDs that were used in a **classified** environment or involved in a spillage incident of **classified** information will be labeled to indicate the classification of the data, the purge date, and the declassified date, as appropriate.

3.7.3.3.5. HDDs used in a classified environment or involved in a spillage incident will never be released outside of DCMA. They will remain under DCMA control until the end of their usefulness and then will be destroyed.

3.7.3.3.6. Only those tools listed on the DCMA Approved Products List will be used to purge HDDs. Only National Security Agency (NSA) approved degaussers will be used to degauss HDDs.

3.7.3.3.7. Contracting officers or agents will include HDD disposition and control measures when either a contractor or vendor provides the service or hardware.

GLOSSARY

DEFINITIONS

The following terminology is chiefly specialized for cybersecurity and CND and is intended for use in this Instruction and the activities described herein. Unless indicated by a parenthetic phrase after the definition that indicates the source publication or document, these terms were documented from CNSSI No. 4009, “National Information Assurance Glossary” (Reference (bi)).

access. Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

access control. The process of granting or denying specific requests: (1) for obtaining and using information and related information processing services; and (2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

Access Control List (ACL). (1) A list of permissions associated with an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. (2) A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.

accreditation. Formal declaration by a DAA or Principal Accrediting Authority that an IS is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization.

administrative control. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

attack sensing and warning. Detection, correlation, identification, and characterization of intentional unauthorized activity with notification to decision makers so that an appropriate response can be developed.

audit. Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures.

audit trail. A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.

authorization (to operate). The official management decision given by a senior organizational official to authorize operation of an IS and to explicitly accept the risk to organizational

operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Authorizing Official (AO). Senior (federal) official or executive with the authority to formally assume responsibility for operating an IS at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

availability. The property of being accessible and useable upon demand by an authorized entity.

backup. Copy of files and programs made to facilitate recovery, if necessary.

biometrics. Measurable physical characteristics or personal behavioral traits used to identify, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics.

Blue Team. 1. The group responsible for defending an enterprise's use of ISs by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).

2. The term Blue Team is also used for defining a group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems.

certification. Comprehensive evaluation of the technical and non-technical security safeguards of an IS to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements. See security control assessment.

Certified TEMPEST Technical Authority (CTTA). An experienced, technically qualified U.S. Government employee who has met established certification requirements IAW CNSS approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

classified information. See classified national security information.

classified national security information. Information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

communications security (COMSEC). A component of IA (i.e., cybersecurity) that deals with measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes crypto security, transmission security, emissions security, and physical security of COMSEC material.

communications security (COMSEC) monitoring. Act of listening to, copying, or recording transmissions of one's own official telecommunications to analyze the degree of security.

community risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

computer network defense (CND). Actions taken to defend against unauthorized activity within computer networks. CND includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

computer network defense (CND) response actions (RAs). CND RAs are deliberate, authorized defensive measures or activities that protect and defend DOD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. RAs extend DOD's layered defense-in-depth capabilities and increase DOD's ability to withstand adversary attacks (CJCSI 6510.01 (Reference (ar))).

COMSEC material. Item designed to secure or authenticate telecommunications. COMSEC material includes, but is not limited to key, equipment, devices, documents, firmware, or software that embodies or describes cryptographic logic and other items that perform COMSEC functions.

confidentiality. The property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.

connection approval. Formal authorization to interconnect ISSs. (DODI 8500.01E, Reference (b)).

contingency plan. Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the COOP or Disaster Recovery Plan for major disruptions.

continuity of operations plan. Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The COOP is the third plan needed by the enterprise risk managers and is used when the enterprise must recover (often at an alternate site) for a specified period of time. Defines the activities of individual

departments and agencies and their sub-components to ensure that their essential functions are performed. This includes plans and procedures that delineate essential functions; specifies succession to office and the emergency delegation of authority; provide for the safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications, and validate the capability through tests, training, and exercises. See also Disaster Recovery Plan and Contingency Plan.

controlled unclassified information (CUI). A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, but is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. The designation CUI replaces the term sensitive but unclassified (SBU). (DODI 5200.01, Reference (ad)).

cybersecurity. Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

cyberspace. A global domain within the information environment consisting of the interdependent network of ISs infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

data integrity. The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.

Defense Information Systems Network. The DoD information resources, assets, and processes required to achieve an information advantage and share information across the Department of Defense and with mission partners. It includes: (a) the information itself and the Department's management over the information life-cycle; (b) the processes, including risk management, associated with managing information to accomplish the DOD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national security systems. (DoDD 8000.01 (Reference (bb))

degauss. Procedure to reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing.

denial of service. The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Department of Defense Information Enterprise. The DOD information resources, assets, and processes required to achieve an information advantage and share information across the

Department of Defense and with mission partners. It includes: (a) the information itself and the Department's management over the information life-cycle; (b) the processes, including risk management, associated with managing information to accomplish the DOD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national security systems. (DoDD 8000.01 (Reference (bb))

Designated Accrediting Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Approval Authority and Delegated Accrediting Authority. (DODI 8500.01 (Reference (b))

enclave. Collection of ISs connected by one or more internal networks under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

firmware. Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.

general support system. An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization.

guard. A mechanism limiting the exchange of information between ISs or subsystems.

incident. An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an IS; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

identification. An act or process that presents an identifier to a system so that the system can recognize a system entity (e.g., user, process, or device) and distinguish that entity from all others.

information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

information assurance (IA). Measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures

include providing for restoration of ISs by incorporating protection, detection, and reaction capabilities.

Information Assurance Manager (IAM). See information systems security manager.

Information Assurance Officer (IAO). See information systems security officer.

Information Assurance Vulnerability Bulletin (IAVB). An IAVB addresses new vulnerabilities that do not pose an immediate risk to DOD systems, but are significant enough that noncompliance with the corrective action could escalate the risk. (CJCSI 6510.01 (Reference (ar))

information environment. Aggregate of individuals, organizations, and/or systems that collect, process, or disseminate information, also included is the information itself.

Information Operation Conditions. The INFOCON system provides a framework within which the Commander USSTRATCOM (CDRUSSTRATCOM), regional commanders, service chiefs, base/post/camp/station/vessel commanders, or agency directors can increase the measurable readiness of their networks to match operational priorities.

information resources. Information and related resources, such as personnel, equipment, funds, and IT.

information security. The protection of information and ISs from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

information system (IS). A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: ISs also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

information system security manager (ISSM). Individual responsible for the IA of a program, organization, system, or enclave.

information system security officer (ISSO). Individual assigned responsibility for maintaining the appropriate operational security posture for an IS or program.

information technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which 1) requires the use of such equipment or 2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers,

ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

integrity. The property whereby an entity has not been modified in an unauthorized manner.

intrusion. Unauthorized act of bypassing the security mechanisms of a system.

major application. An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

major incidents. Root level intrusion providing unauthorized privileged access (Category 1), User level intrusion providing non-privileged access (Category 2), denial of service (Category 4), and new active propagation of malware infecting a DOD IS or malicious code adversely affecting the operations and/or security of DOD IS (Category 7) events or incidents affecting Mission Assurance Category (MAC) I or II DOD ISs. (CJCSI 6510.01 (Reference (ar)),.

malicious logic. Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.

mission partners. Those with whom the Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector.

Mobile Code. Software programs or parts of programs obtained from remote ISs, transmitted across a network, and executed on a local IS without explicit installation or execution by the recipient. **NOTE:** Some examples of software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, ActiveX, VBScript, etc.

National Information Assurance Partnership (NIAP). A U.S. Government initiative established to promote the use of evaluated ISs products and champion the development and use of national and international standards for IT security. NIAP was originally established as collaboration between the National Institute of Standards and Technology (NIST) and the NSA in fulfilling their respective responsibilities under Public Law 100-235 (Computer Security Act of 1987). NIST officially withdrew from the partnership in 2007 but NSA continues to manage and operate the program. The key operational component of NIAP is the Common Criteria Evaluation and Validation Scheme (CCEVS) which is the only U.S. Government-sponsored and endorsed program for conducting internationally-recognized security evaluations of COTS IA and IA-enabled IT products. NIAP employs the CCEVS to provide government oversight or “validation” to U.S. CC evaluations to ensure correct conformance to the International Common Criteria for IT Security Evaluation (ISO/IEC 15408).

network. IS(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

non-repudiation. Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

password. A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data.

personally identifiable information (PII). Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

platform information technology (PIT). IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

platform information technology (PIT) System. A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

policy. A set of principles and associated guidelines to direct and limit DCMA actions in pursuit of objectives, operations, and plans. Establishes Agency-wide rules. Describes the "what," "who," and "why" of operations by defining roles and responsibilities.

procedures. A set of mandatory step-by-step instructions established to implement Agency policy. It describes the process that must be followed to achieve the desired outcome.

protected distribution systems (PDS). Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.

public domain software. Software not protected by copyright laws of any nation that may be freely used without permission of, or payment to, the creator, and that carries no warranties from, or liabilities to the creator.

Public Key Infrastructure (PKI). The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.

remote access (RA). Access to an organization's nonpublic IS by an authorized user (or an IS) communicating through an external, non-organization-controlled network (e.g., the Internet).

risk. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence. **NOTE:** IS-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or ISs and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

risk analysis. Examination of information to identify the risk to an IS. See risk assessment.

risk assessment. The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the RMF.

risk management. The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an IS, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; 3) employment of techniques and procedures for the continuous monitoring of the security state of the IS; and 4) documenting the overall risk management program.

security controls. The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an IS to protect the confidentiality, integrity, and availability of the system and its information.

security inspection. Examination of an IS to determine compliance with security policy, procedures, and practices.

sensitive information. Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, U.S.C. (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information, are to be protected IAW the requirements of the Computer Security Act of 1987 (Public Law 100-235).). See also CUI.

space systems. systems designated as a National Security System (NSS) and/or used to collect, generate, process, store, display, transmit, or receive national security information and/or used to collect, generate, process, store, display, transmit, or receive unclassified information that require security controls to protect it from public release CJCSI 5610.01F (Reference(ar)).

system administrator. Individual responsible for the installation and maintenance of an IS, providing effective IS utilization, adequate security parameters, and sound implementation of established IA (i.e., cybersecurity) policy and procedures.

telecommunication. Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means.

TEMPEST. A name referring to the investigation, study, and control of compromising emanations from telecommunications and automated ISs equipment.

threat. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an IS via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

unauthorized access. Any access that violates the stated security policy.

user. Individual, or (system) process acting on behalf of an individual, authorized to access an IS.

Virtual Private Network (VPN). Protected IS link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.

vulnerability. Weakness in an IS, system security procedures, internal controls, or implementation that could be exploited by a threat source.

vulnerability assessment. Systematic examination of an IS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

GLOSSARY

ACRONYMS

ADP	automated data processing
APO	accountable property officer
AO	authorizing official
ATO	authorization to operate
AUP	Acceptable Use Policy
AV	Anti-Virus
C&A	certification and accreditation
CA	certification authority
CD	compact disk
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMO	Contract Management Office
CND	computer network defense
CNDSP	Computer Network Defense Service Provider
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COMSEC	communications security
COTS	commercial off-the-shelf
CTTA	Certified TEMPEST Technical Authority
CUI	controlled unclassified information
DAA	designated approving authority
DCMA-INST	Defense Contract Management Agency Instruction
DIACAP	Department of Defense Cybersecurity/Information Assurance Certification and Accreditation Process
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	for official use only
FN	foreign national
GFE	government furnished equipment
HDD	hard drives
IA	information assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAVM	Information Assurance Vulnerability Management
IAW	in accordance with

IDS	intrusion detection system
INFOCON	information operations condition
IS	information system
ISO	information system owner
IT	information technology
IT-SLT	Information Technology – Senior Leadership Team
LAN	local area network
LE	Law Enforcement
MAC	mission assurance category
MFR	memorandum for record
MICP	Managers' Internal Control Program
NA	network administrator
NACLC	National Agency Check with Local Agency and Credit Checks
NDA	Non-Disclosure Agreement
NIPRNet	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSTISSP	National Security Telecommunications and Information System Security Policy
NSA	National Security Agency
NOSC	Network Operations and Security Center
OPSEC	operational security
P2P	Peer-to-Peer
PED	portable electronic devices
PII	personally identifiable information
PIT	platform information technology
PKI	public key infrastructure
PM	program/project manager
RA	remote access
RDT&E	research, development, test, and evaluation
RMF	risk management framework
SA	Systems Administrator
SCR	systems change request
SES	Senior Executive Service
SIPRNet	Secret Internet Protocol Router Network
SISO	senior information security officer
SOFA	Status of Forces Agreement
SP	Special Publication
SSBI	single-scope background investigation
STIG	security technical implementation guide

USB universal serial bus
USC United States Code
USSTRATCOM U.S. Strategic Command